3/2012

Datenschutz Nachrichten

35. Jahrgang
ISSN 0137-7767
9,00 Euro

Umfragen

■ Datenschutz im Verlauf von Marktforschungsumfragen ■ Datennutzung in der Hotellerie ■ Europaparlament: Datenschutz-Matinée der DVD ■ Datenschutz im Meldewesen stärken, nicht schwächen ■ Ein Gesetz in nur 57 Sekunden... ■ Pressemitteilung ■ Nachrichten ■ Rechtsprechung ■ Buchbesprechung ■

Deutsche Vereinigung für Datenschutz e.V.
www.datenschutzverein.de

Inhalt

Termine

Montag 8. Oktober 2012 um 19.30 Uhr
Informations- und Diskussionsveranstaltung zur elektronischen Gesundheitskarte
Bornheim (Clubraum 2) Arnsburger Str. 24,
60385 Frankfurt a. M.
(Nähe U-Bahn-Station Höhenstraße Linie U 4).
schaefer@datenschuetz.de

Dienstag, 16. Oktober 2012
Konferenz „Datenschutztag“
Nürnberg.
www.computas.de/konferenzen/it-sa_datenschutz-tag_2012/it_sa_Datenschutztag.html
DVD-Mitglieder erhalten einen 50% Rabatt auf die Teilnahmegebühr.

Mittwoch, 17. Oktober 2012 – Donnerstag, 18. Oktober 2012
Internationale Konferenz
Datenschutz im 21. Jahrhundert
andel’s Hotel Berlin, Landsberger Allee 106, D-10369 Berlin
PGDS@bmi.bund.de

Samstag, 27. Oktober 2012
DVD-Vorstandssitzung
Bonn. Anmeldung in der Geschäftsstelle
dvd@datenschutzverein.de

Sonntag, 28. Oktober 2011
DVD-Mitgliederversammlung
Bonn.

Donnerstag, 1. November 2012
Redaktionsschluss DANA 4/12
Thema: Datenschutzgerechte Webseiten.
verantwortlich: Frans Jozef Valenta
Fragen und Anregungen bitte an:
valenta@t-online.de

Dienstag, 6. November 2012 – Donnerstag, 8. November 2012.
7. dtb-Forum für Arbeitnehmervertreter 2012: „Unsere Daten gehören uns! Mitbestimmung in der digitalen Arbeitswelt“
mit DVD-Beteiligung
Berlin.

Freitag, 9. November 2012
FIfF Jahrestagung 2012
Hochschule Fulda
www.fiff.de

Freitag, 1. Februar 2012
Redaktionsschluss DANA 1/13
Thema: „Löschen“
verantwortlich: Karin Schuler

Editorial

Liebe Leserinnen und Leser,

während wir an diesem Editorial schreiben, feiern die Medien die gelungene Übergabe von 190.000 Unterschriften von Bürgerinnen und Bürgern gegen die Meldegesetznovelle der Bundesregierung. In Zusammenarbeit mit campact und anderen Organisationen hat sich die DVD dem Protest gegen die Vermarktung von Melderegisterdaten angeschlossen und offenbar die Bundesländer überzeugt, die umstrittenen Zugänge der Wirtschaft zu unseren Meldedaten neu zu verhandeln.

In diesem Heft aber soll es auch um ein weiteres ernstes Thema gehen, nämlich den Datenschutz in der Markt- und Meinungsforschung. Ausgewählte Praxisbeispiele dazu und der gewohnte Datenschutznachrichtenteil werden Sie in den nächsten Wochen begleiten – beispielsweise auf dem Weg zu unserer Mitgliederversammlung am 28.10.2012 von 10.00 Uhr bis 13.00 Uhr in Bonn-Bad Godesberg. Der Vorstand wird über seine Jahresaktivitäten berichten, welche uns jüngst nach Brüssel geführt haben, wo wir am 04.09.2012 im Europäischen Parlament zum zweiten Mal eine Datenschutzveranstaltung für und mit Parlamentarierinnen und Parlamentariern veranstaltet haben. Wir freuen uns, Sie zu unserer Mitgliederversammlung begrüßen zu dürfen und wünschen bis dahin einen goldenen, datenschutzfreundlichen Herbst!

Sönke Hilbrans

Autorinnen und Autoren dieser Ausgabe:

Karsten Neumann
Vorstandsmitglied der DVD, Landesbeauftragter für Datenschutz Mecklenburg-Vorpommern a.D., Associate Partner der 2B Advice GmbH,
neumann@datenschutzverein.de

Bettina Rennack
Die Hotelberatung Bettina Rennack ist ein Beratungsunternehmen mit Ausrichtung auf mittelständische und privat geführte Hotels und Restaurants in Mecklenburg-Vorpommern und angrenzenden Regionen. Schwerpunkte sind die Bereiche Qualitätsverbesserung, Weiterbildung und Schulung der Mitarbeiter sowie individuelle Beratungs- und Serviceleistungen.
info@hotelberatung-rennack.de

Timo Wilken
Ass. iur., München, Betrieblicher Datenschutzbeauftragter der in Deutschland zur TNS-Gruppe gehörenden Unternehmen, darunter TNS Infratest und Infratest dimap,
timo.wilken@tns-infratest.com

DANA
Datenschutz Nachrichten
ISSN 0137-7767
35. Jahrgang, Heft 3

Herausgeber
Deutsche Vereinigung für Datenschutz e.V. (DVD)
DVD-Geschäftstelle:
Rheingasse 8-10, 53113 Bonn
Tel. 0228-222498
Konto 1900 2187, BLZ 370 501 98, Sparkasse KölnBonn
E-Mail: dvd@datenschutzverein.de
www.datenschutzverein.de

Redaktion (ViSdP)
Karsten Neumann, Sönke Hilbrans
c/o Deutsche Vereinigung für Datenschutz e.V. (DVD)
Rheingasse 8-10, 53113 Bonn
dvd@datenschutzverein.de
Den Inhalt namentlich gekennzeichneter Artikel verantworten die jeweiligen Autoren.

Layout und Satz
Frans Jozef Valenta, 53119 Bonn
valenta@t-online.de

Druck
Wienands Printmedien GmbH
Linzer Str. 140, 53604 Bad Honnef
wienandsprintmedien@t-online.de
Tel. 02224 989878-0
Fax 02224 989878-8

Bezugspreis
Einzelheft 9 Euro. Jahresabonnement 32 Euro (incl. Porto) für vier Hefte im Jahr. Für DVD-Mitglieder ist der Bezug kostenlos. Das Jahresabonnement kann zum 31. Dezember eines Jahres mit einer Kündigungsfrist von sechs Wochen gekündigt werden. Die Kündigung ist schriftlich an die DVD-Geschäftsstelle in Bonn zu richten.

Leserbriefe
Leserbriefe sind erwünscht. Deren Publikation sowie eventuelle Kürzungen bleiben vorbehalten.

Abbildungen
Frans Jozef Valenta
Seite 115 Campact,
Seite 116 Bundestags-Video,

Timo Wilken

Datenschutz im Verlauf von Marktforschungsumfragen – Ein Überblick aus Sicht der Praxis

Im Verlauf von Befragungen zum Zwecke der Markt-, Meinungs-, Politik-, Rechts- und Sozialforschung (im Folgenden kurz: Marktforschung) erheben, verarbeiten und nutzen Forschungsinstitute personenbezogene Daten, unabhängig davon, ob die Untersuchungen persönlich, schriftlich, online oder telefonisch erfolgen. Die Beachtung des Bundesdatenschutzgesetzes (BDSG) sowie aller anderen datenschutzrechtlichen Bestimmungen stellt dabei ein essentielles Erfordernis, aber auch eine tragende und qualitätssichernde Grundlage der Marktforschung in Deutschland dar. Über allem steht dabei die strikte Wahrung der Anonymität der Befragten.

I. Vor der Befragung

Bereits vor der Beauftragung einer Marktforschungsstudie stellen sich grundlegende datenschutzrechtliche Fragen, die mit den jeweiligen Datenschutzbeauftragten bzw. Rechtsabteilungen der Auftraggeber diskutiert werden sollten. Nicht zu vergessen ist dabei auch eine Aufklärung über die allgemein anerkannten Berufsgrundsätze und Standesregeln[1] sowie den damit verbundenen Anonymitätsgrundsatz.

1. Auftragsdatenverarbeitung oder Funktionsübertragung?

Eine der klassischen Fragen bei der Beauftragung einer Marktforschungsbefragung lautet, ob die Durchführung eine Auftragsdatenverarbeitung nach § 11 BDSG darstellt oder ob nicht vielmehr eine Funktionsübertragung vorliegt. Eine solche liegt vor, wenn die Tätigkeiten des Forschungsinstituts über die Erbringung reiner Hilfsfunktionen hinausgehen und es die übertragenen Aufgaben mit einer gewissen Eigenverantwortlichkeit und Entscheidungsbefugnis durchführt.[2]

Aus Sicht der Praxis liegt bei der Durchführung einer Marktforschungsbefragung regelmäßig eine Funktionsübertragung vor, da diese die tatsächlichen Verhältnisse im Rahmen einer solchen Studie widerspiegelt. Denn eine Auftragsdatenverarbeitung soll datenschutzrechtlich nur dann vorliegen, „wenn der Auftraggeber nicht nur rechtlich, sondern zumindest prinzipiell auch tatsächlich in der Lage ist, dem Auftragnehmer jeden einzelnen Arbeitsschritt vorzuschreiben und letztlich auch die korrekte Durchführung des Datenumgangs kontrollieren zu können."[3] Die Durchführung von Marktforschungsbefragungen erfordert jedoch ein erhebliches fachspezifisches Know-How, das nicht beiläufig zu erwerben ist, sondern das Resultat jahrzehntelanger Erfahrung darstellt; dementsprechend können die aus diesem Know-How resultierenden Handlungsschritte durch den Auftraggeber tatsächlich nicht vollständig angewiesen oder kontrolliert werden. Selbst eine vollständige Darstellung des Studienverlaufes im Rahmen einer Leistungsbeschreibung, dessen Umsetzung dann vom Auftraggeber angewiesen wird, inkludiert regelmäßig nicht sämtliche Erhebungs-, Verarbeitungs- oder Nutzungsvorgänge einer Marktforschungsstudie (z. B. das genaue Procedere der Ziehung einer Stichprobe aus den personenbezogenen Daten).

Weiter soll eine Auftragsdatenverarbeitung dann vorliegen, wenn Dienstleister „lediglich die Kommunikation der Kunden mit der verantwortlichen Stelle vermitteln und dabei im Einzelnen vorgegebene Serviceleistungen ohne eigenen Entscheidungsspielraum erbringen."[4] Als Beispiele dafür werden Call-Center-Leistungen wie die telefonische Entgegennahme von Überweisungsaufträgen oder die Erteilung von Kontoauskünften angeführt. Diese in der Praxis tatsächlich weisungsgebundenen Tätigkeiten mit der Vorbereitung, Durchführung und Auswertung einer Marktforschungsbefragung gleichzusetzen, würde jedoch jeglicher Grundlage entbehren. Denn ein Forschungsinstitut übernimmt i. d. R. die Gesamtdurchführung einschließlich des Befragungs- und Auswertungskonzepts, was wiederum ein Indiz für eine Funktionsübertragung ist. Zudem treten die Forschungsinstitute den Betroffenen in der Kontaktphase des Interviews regelmäßig im eigenen Namen gegenüber, was ebenso als Indiz für eine Funktionsübertragung angesehen wird, wie die Sicherstellung der Betroffenenrechte.[5] Diese erfolgt nämlich – z. B. durch die Sperrung für zukünftige Befragungen – regelmäßig auch durch die Forschungsinstitute.

Im Ergebnis ist daher festzuhalten, dass es sich bei der Durchführung einer Marktforschungsuntersuchung nicht um eine Auftragsdatenverarbeitung handelt, sondern vielmehr um eine Funktionsübertragung. In der Praxis ist es jedoch leider vielfach so, dass die Auftraggeber von einer Auftragsdatenverarbeitung ausgehen und deshalb auf den Abschluss einer entsprechenden Vereinbarung bestehen. Erklärt sich das Forschungsinstitut damit einverstanden, so ist in diese Vereinbarung zumindest aufzunehmen, dass der Auftraggeber keine Weisung erlassen darf, die die Anonymität der Betroffenen gefährdet oder den allgemein anerkannten Berufsgrundsätzen und Standesregeln der deutschen Marktforschung zuwiderläuft. Denn diese sind auch bei einer Beauftragung nach § 11 BDSG zu beachten.[6]

2. § 30a BDSG als Auftragsgrundlage?

Bei dem am 1. September 2009 in das BDSG eingefügten § 30a handelt es sich um eine gesetzliche Erlaubnisnorm i. S. d. § 4 Abs. 1 BDSG für die Marktforschung. Liegen die Voraussetzungen des § 30a Abs. 1 BDSG vor, nämlich dass „kein Grund zu der Annahme besteht, dass der Betroffene ein schutzwürdiges Interesse am Ausschluss der Erhebung, Verarbeitung oder Nutzung hat", ist eine Einwilligung der Betroffenen zur Kontaktierung nicht erforderlich.[7]

Dies stellt eine deutliche Privilegierung der Marktforschung gegenüber der Werbung dar, durch die der Gesetzgeber „den Besonderheiten der Markt- und Meinungsforschung gegenüber der Werbung Rechnung" tragen wollte.[8] Diese Entscheidung ist insbesondere im Hinblick auf die Ermittlung repräsentativer Ergebnisse zu begrüßen. Denn wenn es nur möglich sein sollte, Personen anzusprechen, die gemäß § 4a BDSG ihre Einwilligung gegeben haben, wäre dies mit einem erheblichen zeitlichen und finanziellen Aufwand für die Forschungsinstitute verbunden und die Möglichkeit, repräsentative Ergebnisse ermitteln zu können, deutlich erschwert, wenn nicht gar unmöglich. Der Aufwand für die Betroffenen, einen Widerspruch nach § 30a Abs. 5 i. V. m. § 28 Abs. 4 BDSG mitzuteilen, der von den Forschungsinstituten beachtet werden muss, ist hingegen als gering und als einmalig einzustufen; denn die Forschungsinstitute haben zum einen entsprechende Maßnahmen installiert, die eine erneute Kontaktierung verhindern (siehe Ziff. II. 2.) und zum anderen ein eigenes finanzielles Interesse daran, keine Ordnungswidrigkeit nach § 43 BDSG durch eine erneute Kontaktierung trotz bestehenden Widerspruchs zu begehen.

Zudem nimmt die Markt- und Meinungsforschung eine wichtige gesellschaftliche Aufgabe wahr, wie bereits der Innenausschuss des Deutschen Bundestages in seiner Gesetzesbegründung zur Änderung des BDSG ausgeführt hat: „Sie stellt für öffentliche und private Auftraggeber mittels wissenschaftlicher Methoden und Techniken notwendige Informationen als empirische Grundlage und zur Unterstützung wirtschaftlicher, gesellschaftlicher und politischer Entscheidungen bereit und schafft damit eine wichtige Voraussetzung für die nachhaltige demokratische und wirtschaftliche Entwicklung der Bundesrepublik Deutschland."[9] Daher sei hier noch einmal darauf hingewiesen: Diese Aufgabe könnte durch die Forschungsinstitute bei einem Einwilligungserfordernis nur noch bedingt wahrgenommen werden. In einigen Bereichen wäre Sie de facto unmöglich.

Nicht abschließend geklärt ist bisher die Frage, ob es sich bei § 30a BDSG um eine eigene Auftragsgrundlage handelt und deshalb der Abschluss einer Vereinbarung über eine Auftragsdatenverarbeitung hinfällig ist.[10] Diese von Pflüger[11] vertretene Ansicht, die aus Sicht der Marktforschung zu befürworten wäre, kann mit der vom Gesetzgeber angestrebten Privilegierung der Marktforschung begründet werden: Denn worin ist die Privilegierung zu sehen, wenn das Forschungsinstitut – wie auch bereits vor der Novellierung des BDSG – nur gemäß § 11 BDSG beauftragt werden dürfte? Denn die Nutzung von Adressdaten der Auftraggeber ohne Einwilligung der Betroffenen wäre nach § 11 BDSG auch ohne § 30a BDSG möglich gewesen. Auch könnte argumentiert werden, dass die Marktforschungsinstitute die Adressdaten zum Zwecke der Durchführung einer Marktforschungsbefragung gemäß § 30a BDSG beim Auftraggeber erheben und es somit keines Abschlusses einer Vereinbarung zur Auftragsdatenverarbeitung bedarf.

Im Ergebnis ist daher festzuhalten, dass mit der gesetzlichen Erlaubnisnorm des § 30a BDSG eine eigenständige Auftragsgrundlage geschaffen wurde, aufgrund derer es keines Abschlusses einer Vereinbarung zur Auftragsdatenverarbeitung gemäß § 11 BDSG bedarf. Die technischen und organisatorischen Maßnahmen gemäß § 9 BDSG i. V. m. der Anlage zu § 9 BDSG müssen von den Forschungsinstituten bei einem Auftrag nach § 30a BDSG aber selbstverständlich ebenso erfüllt werden wie bei einer Beauftragung nach § 11 BDSG.

3. Einwilligung der Betroffenen bei telefonischen Kundenzufriedenheitsbefragungen?

Soll das Marktforschungsinstitut eine telefonische Kundenzufriedenheitsbefragung mit anonymisierten Ergebnissen für einen Auftraggeber durchführen, stellt sich eine weitere wesentliche Frage: Handelt es sich bei telefonischen Kundenzufriedenheitsbefragungen um eine unzumutbare Belästigung durch eine geschäftliche Handlung i. S. d. § 7 Abs. 1, 2 Nr. 2 Gesetz gegen den unlauteren Wettbewerb (UWG) und ist daher eine vorherige Einwilligung zur Kontaktierung gemäß § 4 Abs. 1 BDSG erforderlich?

Diese von der Rechtsprechung[12] und Teilen der Literatur[13] überwiegend vertretene Ansicht berücksichtigt jedoch nicht den Willen des Gesetzgebers, der die Marktforschung ohne Differenzierung bei der Erhebungsform durch die Implementierung des § 30a in das BDSG zur Werbung abgrenzen und entsprechend privilegieren wollte (vgl. Ziff. I. 2.). Es fehlt zudem an einer konsequenten Trennung der „mittelbaren Absatzförderung" von der „unmittelbaren Absatzförderung".

Laut UGP-Richtlinie[14] liegt Werbung nur dann vor, wenn eine unmittelbare Absatzförderung gegeben ist. Im Umkehrschluss bedeutet das, dass eine mittelbare Absatzförderung nicht als Werbung zu bezeichnen ist. In der UGP-Richtlinie werden Geschäftspraktiken im Geschäftsverkehr zwischen Unternehmen und Verbrauchern als „jede Handlung (…) die unmittelbar mit der Absatzförderung, dem Verkauf oder der Lieferung eines Produkts an Verbraucher zusammenhängt."[15] Zudem wird in Nr. 26 Satz 1 Anhang zur UGP-Richtlinie, die eine abschließende Aufzählung von unerlaubten Geschäftspraktiken enthält, lediglich der Fall aufgeführt, dass Kunden durch „hartnäckiges und unerwünschtes Ansprechen über Telefon" geworben werden. Wie dies durch einen erstmaligen Anruf geschehen soll, erscheint fraglich.

Die Gesetzesbegründung zum UWG nimmt sich des Verständnisses der UGP-Richtlinie an; demnach unterfallen „weltanschauliche, wissenschaftliche, redaktionelle oder verbraucherpolitische Äußerungen von Unternehmen oder an-

deren Personen (…) weiterhin nicht dem UWG, soweit sie in keinem objektiven Zusammenhang mit dem Absatz von Waren (…) stehen. Dienen sie nur der Information der Leserschaft oder der die Anonymität der befragten Personen wahrenden Markt- und Meinungsforschung, so fehlt es an einem objektiven Zusammenhang zum Warenabsatz, so dass eine geschäftliche Handlung nicht vorliegt.“[16]

Diese strikte Differenzierung in mittelbare und unmittelbare Absatzförderung, die früher regelmäßig zur Trennung von Marktforschung und Werbung herangezogen wurde, wird schlicht übergangen, wenn anonyme Marktforschung mit Werbung gleichgesetzt wird.[17] Sofern als Gegenargumentation die Richtlinie 2006/114/EG[18] herangezogen wird, nach der Werbung „jede Äußerung bei der Ausübung eines Handels (…) mit dem Ziel (…) die Erbringung von Dienstleistungen zu fördern (…)“ sei, ist dem entgegen zu halten, dass den telefonischen Interviews das final angestrebte Ziel des Absatzes gerade fehlt.[19] Denn die Anrufe an sich können und wollen sich nicht unmittelbar auf den Absatz auswirken; möglich wird die mittelbare Absatzförderung – wenn überhaupt – erst durch die ermittelten Studienergebnisse.[20]

Ehmann[21] weist ebenfalls und zurecht daraufhin, dass das Vorliegen einer Absatzförderung nicht ausschließlich damit begründet werden kann, dass eine Marktforschungsbefragung zumindest dadurch mittelbar der Absatzförderung diene, dass sie durch die ermittelten Ergebnisse den jeweiligen Auftraggebern Erkenntnisse für effektivere Werbe- und Absatzförderungsmaßnahmen bereit stelle. Dies träfe nämlich auf nahezu alle Marktforschungsbefragungen zu. Mit dieser Argumentation würde die vom Gesetzgeber vorgesehene Auskoppelung der Markt- und Meinungsforschung aus dem bisherigen § 29 BDSG und die damit intendierte Privilegierung nahezu vollständig unterlaufen.[22]

Diese These wird auch durch die oben zitierte Gesetzesbegründung zum BDSG unterstützt, in der der Gesetzgeber klarstellte, dass die Marktforschung Informationen als empirische Grundlage auch zur Unterstützung wirtschaftlicher Entscheidungen bereitstellt.[23] Dass die Marktforschung zumindest mittelbar der Absatzförderung dient, war dem Gesetzgeber bei seiner Entscheidung, die Marktforschung durch § 30a BDSG zu privilegieren, demnach bewusst. Er hat also auch bewusst die mittelbare Absatzförderung nicht als Werbung definiert und in den Bereich des § 30a BDSG aufgenommen.

Pflüger sieht darüber hinaus die Gefahr, dass – bei konsequenter Anwendung der von der Rechtsprechung vertretenen Ansicht – nahezu jede Marktforschungsbefragung, egal welche Befragungsmethode, unter das Einwilligungserfordernis fällt. Denn die „objektive Feststellung dessen, was ein Unternehmen von seinen derzeitigen und potentiellen Kunden wissen sollte, um im Markt erfolgreich zu sein (…) wird in Form statistischer Ergebnisse geliefert, aus denen die Unternehmen dann erst ihre Schlussfolgerungen zu ziehen haben, also in mittelbarer Form.“[24] Daher wäre nahezu jede Marktforschungsuntersuchung als Werbung zu definieren; die vom Gesetzgeber angestrebte Privilegierung entfiele fast vollständig. Auch sei zu berücksichtigen, dass der deutschen Marktforschung bei dieser Rechtsanwendung ein irreparabler Schaden im internationalen Wettbewerb droht, da es eine solche Regelung nur in Deutschland gäbe.

Die Tatsache, dass von verschiedenen Stimmen in der Literatur die Europarechtskonformität des § 7 Abs. 2 Nr. 2 UWG angezweifelt wird, soll hier nur am Rande erwähnt werden.[25]

Im Ergebnis ist daher festzustellen, dass es sich bei telefonischen Kundenzufriedenheitsbefragungen nicht um Werbung i. S. d. § 7 UWG handelt und eine vorherige Einwilligung der Betroffenen zur Kontaktierung durch das Forschungsinstitut nicht notwendig ist. Die durch den Auftraggeber bei der Implementierung des § 30a BDSG intendierte Privilegierung der anonymen Marktforschung, egal auf Basis welcher Erhebungsmethode, ist bei der rechtlichen Bewertung dieser Anrufe entsprechend zu berücksichtigten.

4. Herkunft der Adressen der zu befragenden Personen?

Bei schriftlichen und Online-Befragungen erhalten die Forschungsinstitute i. d. R. personenbezogene Daten von ihren Auftraggebern gemäß § 30a oder § 11 BDSG oder die Daten werden bei Adresshändlern erhoben. Selbiges kann auch für persönliche oder telefonische Befragungen gelten; jedoch besteht bei den beiden letzteren Befragungsmethoden auch die Möglichkeit, dass diese Adressen durch ein Zufallsverfahren erhoben bzw. „generiert“ werden.

Bei persönlichen Befragungen wird dabei regelmäßig auf das ADM[26]-Master Sample zurückgegriffen; bei diesem Verfahren wird das Gebiet der Bundesrepublik Deutschland in rd. 53.000 Flächen aufgegliedert, in denen es jeweils rd. 700 Privathaushalte gibt. Innerhalb dieser 53.000 Flächen werden über ein Zufallsverfahren eine bestimmte Anzahl zu befragender Haushalte ausgewählt. Anschließend werden bei Mehrpersonenhaushalten erneut über ein Zufallsverfahren (z. B. die Person, die zuletzt Geburtstag hatte) die Personen ermittelt, die befragt werden sollen. Die Reihenfolge der zu befragenden Personen wird anhand eines mathematischen Zufallsverfahrens festgelegt. Dadurch ist sichergestellt, dass eine völlig zufallsgesteuerte Stichprobe entsteht.[27]

Das zuvor beschriebene Verfahren kann bei telefonischen Untersuchungen mangels Telefonverzeichnissen mit sämtlichen tatsächlich vergebenen Rufnummern nicht analog angewandt werden. Daher wurde das Gabler/Häder-Modell als Lösungsansatz entwickelt, auf dem die ADM-Telefonauswahlgrundlagen basieren. Dabei werden zunächst die theoretisch verfügbaren Nummern ermittelt, also solche Nummern, die theoretisch vergeben werden können. Diese wurden von der Bundesnetzagentur festgelegt und sind öffentlich zugänglich. Anschließend werden aus den gesamten theoretisch verfügbaren Nummern 10er-Nummernblöcke für Festnetznummern und 10.000er-Nummernblöcke für Mobilfunknummern gebildet. Über regionale Vorwahlen und ggf. Stadtteilkennnummern kann bei den Festnetznummern eine zufällige regionale Verteilung sichergestellt werden. Aus diesen Blöcken werden dann nach einem Zufallsverfahren diejenigen Rufnummern ausgewählt, die kon-

taktiert werden soll. Ob diese Nummer wirklich verfügbar ist, stellt sich erst beim Kontaktversuch heraus.[28]

Das Verfahren der Rufnummerngenerierung wird datenschutzrechtlich als von § 30a Abs. 1 BDSG erfasst angesehen.[29] Es hat in der Praxis jedoch zur Folge, dass auch solche Rufnummern „generiert“ werden, die nicht in öffentlichen Telefonverzeichnissen enthalten sind und von den Betroffenen häufig als „Geheimnummern“ bezeichnet werden. Entsprechend ungläubig und mitunter ungehalten reagieren die Betroffenen, die als Inhaber einer „Geheimnummer“ angerufen wurden. Daher sind die Telefon-Interviewer im Hinblick auf dieses Problem entsprechend zu schulen, um den Betroffenen eine vernünftige Erklärung liefern zu können.

II. Bei der Befragung

Nachdem die grundlegenden Fragen vor der Beauftragung geklärt sind, ist auch bei der eigentlichen Befragung darauf zu achten, dass die Rechte der Betroffenen ausreichend gewahrt werden.

1. Informationspflichten und Einholung der Einwilligung zur Teilnahme am Interview

Wie bereits dargestellt, stellt § 30a BDSG eine Erlaubnisnorm i. S. d. § 4 Abs. 1 BDSG dar, die eine Einwilligung zur Kontaktierung zu Zwecken der Marktforschung bei Vorliegen der Voraussetzungen des Abs. 1 entbehrlich macht. Weiterhin eingeholt werden muss jedoch selbstverständlich die Einwilligung zur Teilnahme am Interview.

Damit diese Einwilligung rechtmäßig eingeholt wird, ist das Forschungsinstitut gemäß § 4a Abs. 1 Satz 2 BDSG verpflichtet, die Betroffenen rechtzeitig und vollumfänglich über die vorgesehene Verwendung ihrer Daten zu unterrichten, damit diese informiert einwilligen können. Die Betroffenen müssen daher noch vor der Einwilligung zur Teilnahme an der Befragung alle Informationen erhalten, die benötigt werden, um Anlass, Ziel und Folgen der Datenverarbeitung genau einschätzen zu können.[30] Neben dem Institut und dem allgemeinen Zweck der Untersuchung muss den Befragten auch der Auftraggeber mitgeteilt werden, sofern dieser die personenbezogenen Daten der Betroffenen zur Verfügung gestellt hat. Auch der Hinweis auf das Widerspruchsrecht nach § 30a Abs. 5 i. V. m. § 28 Abs. 4 BDSG hat zu erfolgen.[31] Liegen diese Informationen dem Befragten nicht vollständig vor und willigt der Betroffene daraufhin ein, wird die Erhebung, Verarbeitung und Nutzung seiner personenbezogenen Daten rechtswidrig.

Auf eine Besonderheit sei im Hinblick auf telefonische Marktforschungsbefragungen hingewiesen: Einwilligungen bedürfen gemäß § 4a Abs. 1 Satz 3 BDSG regelmäßig der Schriftform. Jedoch ist anerkannt, dass unter besonderen Umständen eine andere Form angemessen sein kann.[32] Ebenso anerkannt ist, dass solch ein besonderer Umstand bei einer telefonischen Marktforschungsbefragung vorliegt, da die Einholung der schriftlichen Einwilligung einen von niemandem erwarteten unzumutbaren Aufwand darstellen würde.[33] Es reicht also die Einholung einer mündlichen Einwilligung aus, die jedoch wohl explizit erfolgen muss.[34]

2. Beachtung von Widersprüchen

Damit ausgeschlossen ist, dass Betroffene nach der Erklärung eines Widerspruchs erneut kontaktiert werden, haben Forschungsinstitute Sperrlisten zu führen, in die die sog. „Absolutverweigerer“ eingetragen werden. Stichproben, die für eine Umfrage genutzt werden sollen, müssen vor Beginn der Feldarbeit und sodann laufend mit den tagesaktuellen Sperrlisten abgeglichen werden, um eine erneute Kontaktierung eines Betroffenen, der einen Widerspruch geltend gemacht hat, auszuschließen.

Für den Fall telefonischer Befragungen hat der ADM eine zentrale Sperrdatei installiert; der Schutz der Betroffenen geht dabei sogar über die gesetzliche Pflicht des § 30 Abs. 5 i. V. m. § 28 Abs. 4 BDSG hinaus: Obwohl nur das Institut, dem gegenüber der Betroffene seinen Widerspruch erklärt hat, verpflichtet ist, diesen zu beachten, wird der Widerspruch durch die ADM-Sperrdatei von allen ADM-Mitgliedsinstituten, die einen Abgleich mit dieser Sperrdatei vornehmen, beachtet. Gestützt werden kann die Sperrdatei (und damit auch die institutseigenen Sperrlisten) laut Ehmann auf § 29 Abs. 1 Satz 1 Nr. 1 BDSG, da ein Marktforschungsinstitut ein erhebliches Interesse daran habe, seiner Pflicht aus § 30a Abs. 5 i. V. m. § 28 Abs. 4 BDSG nachzukommen; ein Betroffener, der der Teilnahme an zukünftigen Marktforschungsbefragungen für die Zukunft widersprochen hat, habe hingegen kein schutzwürdiges Interesse daran, nicht in eine solche Sperrdatei eingetragen zu werden; denn diese diene dazu, sein erklärtes Ziel, nämlich zukünftige telefonische Kontaktierungen für Marktforschungszwecke, in großem Umfang zu unterbinden.[35]

3. Information des Auftraggebers über Widersprüche

Teilt ein Betroffener bei einer Befragung seinen Widerspruch nach § 30a Abs. 5 BDSG i. V. m. § 28 Abs. 4 BDSG mit, stellt sich für das Forschungsinstitut die Frage, ob der Auftraggeber über diesen Widerspruch informiert werden muss.

Hierbei sind zwei Fälle zu unterscheiden: Richtet sich der Widerspruch nur gegen das die Untersuchung durchführende Institut, muss der Befragte im Forschungsinstitut gesperrt werden. Richtet sich der Widerspruch aber generell gegen die Erhebung, Verarbeitung oder Nutzung der Daten für Zwecke der Marktforschung, ist das Forschungsinstitut darüber hinaus verpflichtet, neben der Sicherstellung der Sperrung im Institut auch die Stelle zu informieren, die für die Übermittlung der Daten verantwortlich ist, damit eine Sperrung auch bei dieser Stelle ermöglicht wird.[36]

Zudem werden die Befragten in der konkreten Interviewsituation häufig nicht in der Lage sein, zwischen Auftraggeber und Forschungsinstitut zu unterscheiden und einfach nur darum bitten, nicht mehr angerufen zu werden. Daher erscheint es deshalb auch in diesen Fällen richtig, dass das Forschungsinstitut den Widerspruch an die Stelle, die die Daten übermittelt hat, unverzüglich weiterleiten muss.

4. Einholung der Einwilligung in Folge- oder Wiederholungsbefragungen

Mitunter kann es bei bestimmten Untersuchungskonzepten notwendig werden, dieselben Personen zu einem bestimmten Thema noch einmal zu befragen (Folgebefragung) bzw. nach einem zeitlichen Abstand denselben Personen exakt die gleichen Fragen erneut zu stellen (Wiederholungsbefragung) und dabei auf die Ergebnisse der vorherigen Befragung zurückzugreifen, um z. B. Veränderungen in bestimmten Markt- und Lebenssituationen zu messen.

Für die Teilnahme an einer sog. Folge- oder Wiederholungsbefragung muss das Forschungsinstitut eine informierte Einwilligung der Betroffenen zur Teilnahme an dieser Befragung und die damit verbundene Speicherung der Adress- und Befragungsdaten vom Befragten einholen. Die Adress- und Befragungsdaten müssen in diesen Fällen getrennt voneinander aufbewahrt werden und dürfen nur über eine Codenummer verbunden sein. Eine Wiederzusammenführung darf nur für die Folge- oder Wiederholungsbefragung erfolgen. Zudem dürfen die Daten für keinen anderen Zweck verwendet werden.[37]

III. Nach der Befragung

Auch nach der Durchführung der Befragung sind weiterhin datenschutzrechtliche Verpflichtungen zu erfüllen; dazu gehört insbesondere die schnellstmögliche Trennung der Adress- und Befragungsdaten und damit die Sicherstellung der Einhaltung des Anonymitätsgrundsatzes.

1. Anreichern von Daten

Häufig werden nach Abschluss der Befragung noch allgemein zugängliche Informationen an den erhobenen Datensatz angereichert. Die Standesregeln erlauben die Anreicherung, wenn das Forschungsziel dies erfordert und die Anonymität der untersuchten Personen gegenüber dem Auftraggeber gewahrt bleibt.[38] Eine Anreicherung von Daten ist als „Verändern" i. S. d. § 3 Abs. 4 Nr. 2 BDSG anzusehen, also „das inhaltliche Umgestalten gespeicherter Daten". Damit ist jede Maßnahme gemeint, durch die der Informationsgehalt des Datensatzes geändert wird.[39] Datenschutzrechtlich ist diese Anreicherung nicht zu beanstanden; sie ist durch § 30a Abs. 2 BDSG gedeckt.[40]

2. Pseudonymisierung

Die bei einer Marktforschungsbefragung erhobenen Daten müssen im Forschungsinstitut pseudonymisiert werden, sobald dies nach dem Zweck des Forschungsvorhabens, für das diese Daten erhoben worden sind, möglich ist. Gemäß § 3 Abs. 6a BDSG ist das Pseudonymisieren „das Ersetzen des Namens und anderer Identifikationsmerkmale durch ein Kennzeichen zu dem Zweck, die Bestimmung des Betroffenen auszuschließen oder wesentlich zu erschweren".

Bei einer Pseudonymisierung werden die Adress- und Befragungsdaten getrennt voneinander gespeichert und mit identischen Code-Nummern versehen, um diese Daten wieder zusammenführen zu können. Bei einer einmaligen Befragung geschieht das lediglich vorübergehend und ausschließlich zu Zwecken der Qualitätskontrolle; bei Folge- oder Wiederholungsbefragungen können darüber hinaus auch die Erhebungsdaten aus den verschiedenen Interviews – eine entsprechende Einwilligung der Betroffenen vorausgesetzt (vgl. Ziff. II. 4.) – bis zum Abschluss der Gesamtuntersuchung miteinander verknüpft werden.[41] Nach Abschluss der Gesamtuntersuchung werden die personenbezogenen Adressdaten umgehend gelöscht.

3. Anonymisierung

In den Standesregeln der Berufsverbände[42] in Deutschland ist die Pflicht zur Anonymisierung der personenbezogen erhobenen Befragungsdaten bereits seit Jahrzehnten enthalten.[43] Seit der BDSG-Novelle vom 1. September 2009 ist diese Pflicht nun auch gesetzlich in § 30a Abs. 3 BDSG verankert. Dies ist zu begrüßen, da der Zweck der Marktforschung ausschließlich in der Ermittlung verallgemeinerungsfähiger Aussagen über die Bevölkerung bzw. bestimmte Teile der Bevölkerung sowie über Unternehmen bzw. Institutionen liegt. Die häufig von Auftraggebern angefragte individuelle Nutzung von personenbezogenen Einzelangaben ist nach den Standesregeln der Markt- und Sozialforschung strikt untersagt.[44]

Zu beachten ist bei der Anonymisierung insbesondere, dass nicht nur die „reinen" personenbezogenen Daten (wie z. B. Vorname und Nachname) zur Identifikation der Befragten führen können und daher nicht an den Auftraggeber oder sonstige Dritte übermittelt werden dürfen, sondern auch die Möglichkeit der Bestimmbarkeit durch weitere Merkmale (z. B. der Beruf „Bundeskanzlerin") bzw. deren Verknüpfung (z. B. wenn es nur eine professionelle Cellistin im Alter zwischen 40 und 50 Jahren im Stadtteil Wedding in Berlin gibt) verhindert werden muss. Dies ist insbesondere dann problematisch, wenn ein Auftraggeber einen Datensatz mit anonymisierten Einzelinterviews verlangt. Hier trifft das Forschungsinstitut die Pflicht zu prüfen, ob aufgrund einzelner bzw. der Verbindung einzelner Merkmale eine Identifizierung der Befragten ausgeschlossen ist. Ergibt die Prüfung, dass eine Identifizierung einzelner Befragter möglich ist, muss das Forschungsinstitut die Merkmale, die zu einer Identifizierung führen, aus dem Datensatz entfernen. Auch hier gilt: Der Anonymitätsgrundsatz als Wesen der Marktforschung in Deutschland ist zwingend einzuhalten.

IV. Fazit

Der Datenschutz spielt bei der Durchführung von Marktforschungsuntersuchungen eine wichtige Rolle. Dies beginnt bereits vor der eigentlichen Befragung und setzt sich bis zum Zeitpunkt der Anonymisierung nach der Befragung fort. Die bestehenden datenschutzrechtlichen Probleme werden voraussichtlich nicht ab-, sondern vielmehr zunehmen. Themen wie Befragungen via Social Media, Cookie-Analysen etc. werden neue Herausforderungen darstellen, denen sich die Marktforschungsbranche datenschutzrechtlich stellen und einen Spagat zwischen dem Bedürfnis nach innovativen

Forschungsmethoden und -kanälen einerseits sowie der Einhaltung sämtlicher Bestimmungen zum Datenschutz andererseits hinbekommen muss. Es bleibt also spannend.

1 Der Autor ist Volljurist und als betrieblicher Datenschutzbeauftragter der in Deutschland zur TNS-Gruppe gehörenden Unternehmen, darunter TNS Infratest und Infratest dimap, bestellt.

Abrufbar auf der Homepage des Arbeitskreises Deutscher Markt- und Sozialforschungsinstitute e. V. (ADM) unter http://www.adm-ev.de.

2 Wedde in Däubler/Klebe/Wedde/Weichert, Bundesdatenschutzgesetz, 3. Aufl., § 11, Rdnr. 14.

3 Petri in Simitis [Hrsg.], BDSG, 7. Aufl., § 11, Rdnr. 20.

4 Petri in Simitis [Hrsg.], § 11, Rdnr. 29.

5 Vgl. dazu Petri in Simitis [Hrsg.], § 11, Rdnr. 23.

6 Vgl. dazu Richtlinie zum Umgang mit Adressen in der Markt- und Sozialforschung, Ziff. 4.5.

7 Gola / Schomerus, BDSG, 10. Aufl., § 30a, Rdnr. 2; Bergmann/Möhrle/Herb, Datenschutzrecht, § 30a, Rdnr. 3; Pflüger, Datenschutz in der Markt- und Meinungsforschung, RDV 2010, 101, 102.

8 BT-Drs. 16/13657, S. 33.

9 BT-Drs. 16/13657, S. 19 f.

10 Gola / Schomerus, § 11, Rdnr. 9.

11 Pflüger, RDV 2010, 101, 102.

12 OLG Köln, Urteil vom 30. März 2012, 6 U 191/11; OLG Köln, Urteil vom 12. Dezember 2008, 6 U 41/08; OLG Stuttgart, GRUR 2002, 457, 458.

13 Köhler in Köhler/Bornkamm, UWG, 30. Auflage, 2012, § 7, Rdnr. 133.

14 Richtlinie 2005/29/EG des Europäischen Parlaments und des Rates vom 11. Mai 2005 über unlautere Geschäftspraktiken zwischen Unternehmen und Verbrauchern.

15 UGP-Richtlinie 2005/29/EG, S. 26.

16 Änderungsgesetz vom 22. Dezember 2008 (BGBl I, Seite 2949).

17 Vgl. dazu Schweizer, Grundsätzlich keine Anwendbarkeit des UWG auf die Medien- und insgesamt auf die Markt- und Meinungsforschung, ZUM 2010, 400.

18 Richtlinie 2006/114/EG des Europäischen Parlaments und des Rates vom 12. Dezember 2006 über irreführende und vergleichende Werbung, Art. 2 lit. a, S. 22.

19 Vgl. dazu Engels / Brunn, Wettbewerbsrechtliche Beurteilung von Kundenzufriedenheitsbefragungen, WRP 2010, 687, 688.

20 So auch Haug, Stellen Anrufe zur Kundenzufriedenheitsermittlung oder der Werbezustellungskontrolle Telefonwerbung dar?, K&R 2010, 767, 769.

21 Ehmann in Simitis [Hrsg.], § 30a, Rdnr. 41.

22 Siehe auch Pflüger, RDV 2010, 101, 103 f.

23 Änderungsgesetz vom 22. Dezember 2008 (BGBl I, Seite 2949).

24 Vgl. dazu Pflüger, RDV 2010, 101, 104 f.

25 Vgl. z. B. Engels / Brunn, Ist § 7 II Nr. 2 UWG europarechtswidrig?, GRUR 2010, 886.

26 Arbeitskreis Deutscher Markt- und Sozialforschungsinstitute e. V.

27 Eine ausführliche Beschreibung ist abrufbar auf der Internetseite des ADM (www.adm-ev.de) unter „ADM-Stichprobe“ > „Die ADM-Stichproben für persönlich-mündliche Befragungen“.

28 Eine ausführliche Beschreibung ist abrufbar auf der Internetseite des ADM (www.adm-ev.de) unter „ADM-Stichprobe“ > „Die ADM-Stichproben für telefonische Befragungen“.

29 Ehmann in Simitis [Hrsg.], § 30a, Rdnr. 114.

30 Simitis in Simitis [Hrsg.], § 4a, Rdnr. 70.

31 Richtlinie zum Umgang mit Adressen in der Markt- und Sozialforschung, Ziff. 5 Abs. 2.

32 Gola / Schomerus, § 4a, Rdnr. 13.

33 Däubler in Däubler/Klebe/Wedde/Weichert, § 4a, Rdnr. 15; Gola / Schomerus, § 4a, Rdnr. 13.

34 Simitis in Simitis [Hrsg.], § 4a, Rdnr. 43 f.

35 Ehmann in Simitis [Hrsg.], § 30a, Rdnr. 146.

36 Richtlinie zum Umgang mit Adressen in der Markt- und Sozialforschung, Ziff. 5 Abs. 3.

37 Richtlinie zum Umgang mit Adressen in der Markt- und Sozialforschung, Ziff. 4.7.2.

38 Richtlinie zum Umgang mit Adressen in der Markt- und Sozialforschung, Ziff. 6.3.

39 Dammann in Simitis [Hrsg.], § 3, Rdnr. 129.

40 Ehmann in Simitis [Hrsg.], § 30a, Rdnr. 137; Weichert in Däubler/Klebe/Wedde/Weichert, § 30a, Rdnr. 4.

41 Richtlinie zum Umgang mit Adressen in der Markt- und Sozialforschung, Ziff. 3.5.2.

42 Arbeitskreis Deutscher Markt- und Sozialforschungsinstitute e. V. (ADM), Arbeitsgemeinschaft Sozialwissenschaftlicher Institute e. V. (ASI), Berufsverband Deutscher Markt- und Sozialforscher e. V. (BVM), Deutsche Gesellschaft für Online-Forschung e. V. (DGOF).

43 Richtlinie zum Umgang mit Adressen in der Markt- und Sozialforschung, Ziff. 3.5.1.

44 Vgl. dazu Ziff. 4 der „Erklärung für das Gebiet der Bundesrepublik Deutschland zum ICC/ESOMAR Internationalen Kodex für die Markt- und Sozialforschung“.

Bettina Rennack

Datennutzung in der Hotellerie – Gästebefragungen als Teil des Qualitätsmanagements

Ziel eines jeden Unternehmers – auch des Hoteliers – ist die Erwirtschaftung von Gewinn. Dies erreicht der Hotellier, wenn er zusammen mit seinen Mitarbeitern seine Kernaufgaben beherrscht – nämlich herausragende Serviceleistungen für den Gast zu erbringen und überdurchschnittliche Umsätze in den verschiedenen Bereichen des Hotels zu generieren. Voraussetzung hierfür sind neben einem guten Produkt am richtigen Standort vor allem betriebswirtschaftlicher Sachverstand, strategisches Denken und Handeln, Organisationsvermögen und der eigene Qualitätsanspruch, der sich letztlich in der Klassifizierung des Hauses auch nach Außen wiederspiegeln muss.

Neben diesen Kernaufgaben und allen erforderlichen Maßnahmen für Qualitätssicherung, Produkt- und Weiterentwicklung oder neuen Marketing-Strategien stürmt noch eine Vielzahl von Themen auf den Hotelier ein. Mancher sieht sich mitunter sogar am Gängelband der Institutionen, wenn er sich mit Themen wie GEMA, Bettensteuer, Hygiene-Ampel, GEZ-Gebühren, Tariflohn und zusätzlich auch noch mit datenschutzrechtlichen Bestimmungen auseinandersetzen muss.

Dennoch ist dabei der Hotelier in einer von Vielen beneideten Situation. Denn er gelangt wie kaum ein Unternehmer anderer Branchen zu derart vielen persönlichen Daten und Informationen über den Kunden/Gast, die vollständige Profile ergeben und für die Gästebindung genutzt werden können und auch wollen.

Der Hotelier gelangt ohne besonderen Aufwand durch Reservierung über Check-In, Aufenthalt, Check-Out bis zur After-Sales-Phase zu einer Vielzahl von Informationen über den Gast. Diese stehen teilweise in unmittelbarem Zusammenhang mit der Vertragsabwicklung (Beherbergungsvertrag), teilweise werden sie aber auch zusätzlich bewusst in Gesprächen mit Gästen gewonnen, dokumentiert und für die Sicherstellung der Kundenzufriedenheit oder für Werbemaßnahmen genutzt. Der Hotelier weiß vom Gast außer den unmittelbaren Kontaktinformationen oftmals aus den Gesprächen mit ihm auch ganz persönliche Daten wie Hochzeitstag, Namen der Kinder oder des Hundes, Allergien und Unverträglichkeiten, sportliche Aktivitäten oder Gourmet-Vorlieben. Nutzt der Hotelier diese Daten, fühlt sich der Gast oft ganz persönlich angesprochen.

Wie gelangt der Hotelier an weitere Daten und vor allem, was geschieht mit den so gesammelten Daten?

Seine Möglichkeiten bzw. auch der Aufwand hierfür variiert von Haus zu Haus und hängt vielfach von der vorhandenen Manpower ab. Während das kleine Hotel mit nur wenigen Mitarbeitern sich eher auf klassische Fragebögen konzentriert, suchen die großen Häuser zusätzlich eine Vielzahl von persönlichen Kontakten. Das Zusammentreffen von Gästen und auf Kundenbindung spezialisierten Mitarbeitern findet in Form von Begrüßungsrunden mit Hausführung und anschließendem Glas Sekt bis hin zum Small-Talk mit dem Hoteldirektor statt.

Die klassische Variante bleibt jedoch immer noch die Gästebefragung in Form eines Fragebogens. Hier wird der Gast aufgefordert, die Leistungen des Hotels in den Bereichen Reservierung, Rezeption, Hotelzimmer, Restaurant, Freizeit und sonstiger Leistungen anhand einer Bewertungsskala zu beurteilen. Der Fragebogen lässt im Allgemeinen auch ausreichend Raum, um persönliche Anregungen oder auch Beschwerden vorzutragen. Für die Optimierung der Kundenzufriedenheit sind vor allem die negativen Bewertungen und Anregungen durch die Gäste von Bedeutung. Natürlich ist es dem Hotelier wichtig zu wissen, wer der Verfasser eines Fragebogens ist, kann er doch unmittelbar zu den Beanstandungen Stellung nehmen. Dies nimmt auch der Gast wohlwollend zur Kenntnis.

Wer sich in seinem Kundenbindungsmanagement von der Masse der Hotels absetzen möchte, bevorzugt individuelle Kontakte, um ganz spezifische Informationen zu erhalten. In Gesprächsführung besonders geschulte Mitarbeiter kommen in angenehmer Atmosphäre mit Hotelgästen zusammen um zu plaudern, für Fragen zur Verfügung zu stehen oder sich der Dinge, mit denen der Gast unzufrieden ist, anzunehmen. Ob Guest-Relation, Front-Office oder Sales – die Mitarbeiter dieser Abteilungen dokumentieren alles Wesentliche in der Kundendatenbank. Die weitere Verwendung dieser Gastdaten dient zum Ausbau der Kundenzufriedenheit, zur Vorbeugung erneuter Beschwerdesituationen oder zum gezielten Marketing. Je spezifischer die Daten sind, umso gezielter kann das Marketing des Hauses ansetzen und verhindert dabei mögliche Streuverluste.

Alternativ zu den eigenen Gästebefragungen bietet natürlich auch eine Vielzahl von Bewertungsportalen dem Hotelier Erkenntnisse, wie zufrieden Gäste mit seinem Produkt und seinen Serviceleistungen sind. Für viele Hoteliers sind Bewertungsportale Fluch und Segen zugleich. Sie bieten potentiellen Gästen eine Hilfestellung in der Entscheidung für oder gegen ein Hotel. Bei einer hohen Weiterempfehlungsquote ist das Bewertungsportal ein gutes Marketing-Instrument. Negativ zu beurteilen ist aber dennoch der immer noch mögliche Missbrauch. Denn auch ohne

tatsächlich Gast in einem Hotel gewesen zu sein, kann eine Bewertung ohne großen Aufwand abgegeben werden. Zum möglichen Schaden des Hoteliers.

Anders zu betrachten sind jene Hotelbewertungen, die über Reservierungsportale veröffentlicht werden. Hier ist die Verlässlichkeit für den Hotelier (und für den potenziellen Kunden) größer, da eine Bewertung eines Hotels nur möglich ist, wenn der Aufenthalt auch tatsächlich stattgefunden hat.

Ein vergleichbares Verfahren bieten große Hotels oder Hotelketten, die den Gast nach Rückkehr, falls noch kein Gästefragebogen ausgefüllt wurde, um eine Hotelbewertung bitten. Über einen Link gelangt der Gast dann zu einem unabhängigen Partner für Hotelbewertungen.

Über den Nutzen von Gästebefragungen oder die Sinnhaftigkeit von Bewertungsportalen gibt es sicher unterschiedliche Betrachtungen, allemal zwischen Datenschützern und Hoteliers. Wo sich die Einen um Gefahren und möglichen Missbrauch von Gastdaten sorgen, kümmern sich die Anderen um die Einhaltung von Vorgaben, die innerhalb bestimmter Hotelkategorien bestehen. Die Deutsche Hotelklassifizierung, die für die Vergabe der Hotelsterne einen Kriterienkatalog (aktuelle Version 2010 – 2014) zugrunde legt, der die Standards in den verschiedenen Kategorien sicherstellt, setzt auch beim Thema Gästebefragung gewisse Maßstäbe. Strebt ein Hotel eine Klassifizierung zum 4 Sterne- oder 5 Sterne-Hotel an, ist die Durchführung systematischer Gästebefragungen ein Mindestkriterium. Genauer heißt es: „Hierunter ist das aktive und systematische Einholen und Auswerten von Gästemeinungen zur Qualität der erbrachten Hotelleistungen (z.B. durch Befragungsbögen / -karten) und der darauf folgende Abbau etwaiger betrieblicher Schwachstellen und die Umsetzung von Verbesserungsvorschlägen zu verstehen.“

Wer in dieser Kategorie keine Gästebefragungen durchführt, kann von der Sterne-Plakette am Hoteleingang nur träumen.

Eine ganz andere Form, sich der Qualität der eigenen Leistung zu vergewissern ist die Durchführung eines professionellen Mystery guestings. In Absprache mit der Hotelleitung überprüft ein darauf spezialisierter Anbieter die Leistungen des Hotels. Anhand eines festgelegten Kriterienkataloges werden in allen Bereichen (von der Reservierung bis zur Abreise) die Angebots-, Ausstattungs- und Servicequalität, interne und externe Betriebsabläufe sowie das Preis-Leistungs-Verhältnis bewertet. Die Hotelleitung erhält im Anschluss an den so genannten Mystery-Check einen ausführlichen Prüfbericht mit Empfehlungen. Die Mitarbeiter des Hotels haben von der Tätigkeit des Gastes/Testers keine Kenntnis.

Auch hier mag sicher der Bedenkenträger wieder Schlimmes befürchten. Doch wie schon bei der Gästebefragung gilt es auch beim Mystery guesting, einen Blick auf die Vorgaben zur Hotelklassifizierung zu werfen. In den gehobenen Hotelkategorien 4 Sterne-Superior und 5 Sterne ist es verpflichtend, das Hotel von einem externen Prüfer testen zu lassen. Genauer heißt es: „Mystery guestings müssen von spezialisierten Drittanbietern auf Initiative und Rechnung des Hotels mindestens einmal innerhalb des Klassifizierungszeitraumes durchgeführt werden, ausgewertet und dokumentiert werden. Verdeckte Eigenkontrollen durch Hotelketten oder Hotelkooperationen sind als gleichwertig zu betrachten.“

Kundenbindung also versus Datenschutz!? Kundenbindung und Kundenzufriedenheit als eine der größten Herausforderung der Branche beruht auf verfüg- und nutzbaren Gastdaten. Dies wird mit Blick auf die Wettbewerbslage immer wichtiger, so dass als Konsequenz auch die zu verarbeitenden Daten nach Art und Menge zunehmen. Die Sensibilisierung vieler Gäste für diese Thematik hat zu einer deutlichen Zunahme von Datenschutzerklärungen seitens der Hotellerie geführt. Die renommierten Häuser haben hier längst gehandelt. Aber auch die kleineren Hotels sind zunehmend auf dem richtigen Weg. Bleibt nur die technische Herausforderung, die jeweilige Hotelsoftware so zu konfigurieren, dass das System für die Marketing-Aktivitäten zwischen Einwilligungserklärung und Widerruf des Gastes unterscheiden kann.

Karsten Neumann

Europaparlament: Datenschutz-Matinée der DVD


Europaparlament – Brüssel

Nachdem die DVD am 19. Oktober 2011 eine erste Fachdiskussion zum Thema Beschäftigtendatenschutz im Europaparlament in Brüssel mit viel Erfolg durchgeführt hatte, war eine Fortsetzung dieses Angebotes für die Europaparlamentarier verabredet worden. Dieses fand am 4. September wieder im Europaparlament statt, diesmal auf Einladung der Europaabgeordneten Birgit Sippel, Fraktion der Progressiven Allianz der Sozialisten und Demokraten im Europäischen Parlament (Sozialdemokraten). Die Veranstaltung widmete sich den im Entwurf für eine Datenschutzgrundverordnung (DSGVO) vorgesehenen Kontrollinstrumenten.

Was uns bei der Vorbereitung der Veranstaltung nicht so ganz klar war, machte sich bei den Teilnehmerzahlen bemerkbar: Der Veranstaltungstag war erst der zweite Arbeitstag des Europaparlaments nach der Sommerpause, die Veranstaltung musste wegen Baufälligkeit eines Gebäudeteils kurzfristig in einen anderen Sitzungssaal verlegt werden und die Arbeitskampfmaßnahmen bei einer deutschen Fluggesellschaft wirkten sich ebenfalls negativ aus. Dafür war das Interesse der Datenschutzpolitiker aller Fraktionen groß: die großen Fraktionen waren prominent in der ersten Runde der Matinée mit den sog. Schattenberichterstattern zur DSGVO vertreten. Mitarbeiterinnen und Mitarbeiter der Fraktionen, der Kommission und des Europäischen Datenschutzbeauftragten konnten eine detailreiche und konstruktive Informations- und Diskussionsveranstaltung zu einem der gegenwärtig größten Gesetzgebungsvorhaben erleben.


Birgit Sippel, MdEP

Frau Birgit Sippel eröffnete die Matinée mit einem deutlichen Lob an den engagierten Versuch der Vizepräsidentin Reding, mit ihrem Entwurf europaweit einheitlich hohe Datenschutzstandards zu schaffen. Die Parlamentarier seien sich in dieser Zielstellung fraktionsübergreifend einig. Allerdings beginne jetzt erst der Diskussionsprozess, in dem viele Fragen beantwortet und Kompromisse gefunden werden müssten. Vor allem die vorgesehenen Regulierungsrechte der Kommission würden von den Abgeordneten besonders kritisch gesehen. Angesichts der zunehmenden Komplexität des Themas bräuchte es für alle Betroffenen verlässliche, klare und möglichst vollständige gesetzliche Regelungen. Die Datenschutz-Matinée der DVD leitete damit die parlamentarischen Beratungen des Kommissionsentwurfes ein, die in den nächsten Monaten die Arbeit des zuständigen Ausschusses bestimmen werden.


Jan Philipp Albrecht, MdEP

Der Berichterstatter des Europäischen Parlaments, der Grünen-Abgeordnete Jan Philipp Albrecht, eröffnete die Reihe der Statements mit einem deutlichen Hinweis auf die Größe der anstehenden Aufgabe. Das Parlament wird zuerst unter den nationalen und politischen Interessen der Abgeordneten und anschließend mit den Vertretern der 27 nationalen Regierungen, also dem Rat, einen Kompromiss aushandeln müssen. Dabei habe sich das Parlament in der Stellungnahme des damaligen Berichterstatters Axel Voss zum Datenschutz-Gesamtkonzept bereits auf vier Kernforderungen geeinigt: eine europaweit einheitlich verbindliche Regelung, die ein hohes Datenschutzniveau durch einen hohen Grad an Harmonisierung mit dem Ziel der Rechtssicherheit festlegt, die Betroffenenrechte stärkt und effektive Sanktionsmöglichkeiten enthält. Auch Albrecht sieht neben einer Reihe von positiven Vorschlägen zur Stärkung der Auskunftsrechte und

Informationspflichten die sog. delegierten Rechtsakte – eine Form von Verordnungsermächtigung für die Kommission – als problematisch an. Die Anzahl von Mitarbeitern als Schlüssel für die Bestellungspflicht eines Datenschutzbeauftragten (der Entwurf sieht diese erst bei 250 Mitarbeitern vor) hält er generell für ungeeignet. Sein Ziel sei es, in dieser Frage auch Rechtssicherheit für die Unternehmen zu erreichen. Vom bisherigen Gang der Diskussion berichtet Albrecht über eine große Zahl von Unternehmensvertretern und -lobbyisten, die sich personalintensiv Gehör verschaffen. Die Begleitung dieses Prozesses aus der Verbraucher- und der Datenschutzperspektive sei auch deshalb enorm wichtig, um ein ausgeglichenes Ergebnis zu erreichen.


Axel Voss, MdEP

Der Schattenberichterstatter der Fraktion der Europäischen Volkspartei (Christdemokraten) Axel Voss verwies auf die Schwierigkeit, eine Lösung für Alles erreichen zu wollen. Jedes Geschäftsmodell müsse sich möglichst mit ausgeglichenen Regelungen in der Datenschutzgrundverordnung wiederfinden. Technisch bedingt sei mit der modernen Informations- und Kommunikationstechnik ein enormes Ungleichgewicht zwischen Anbieter und Nutzer entstanden. Sein Ziel sei es daher, für mehr Gleichgewicht und Rechtssicherheit für Unternehmen, Betroffene und die öffentliche Verwaltung zu sorgen. Dem genüge der gegenwärtige Text noch nicht, da er zu viele Interpretationsspielräume eröffne. Auch er könne schon aus dem parlamentarischen Selbstverständnis heraus die Fülle an delegierten Rechtsakten nicht akzeptieren. Die Verordnung solle Anreize für die Bestellung betrieblicher Datenschutzbeauftragter schaffen und das Verhältnis der Haftung zwischen der verantwortlichen Stelle und dem Auftragsdatenverarbeiter konkretisieren. Ebenso müsse die in Artikel 7 Absatz 4 vorgesehene Regelung konkretisiert werden, wonach bei einem erheblichen Ungleichgewicht zwischen den Positionen der betroffenen Person und der verantwortlichen Stelle eine Einwilligung keine wirksame Rechtsgrundlage darstellen solle.


Alexander Alvaro, MdEP

Auf den Zeitrahmen der Diskussion bis Mitte 2014 „ob wir wollen oder nicht" wies der Vizepräsident und Abgeordnete Alexander Alvaro, Fraktion der Allianz der Liberalen und Demokraten für Europa, hin. Trotz der momentanen Einigkeit zwischen den Fachpolitikern der Fraktionen sei dies eine anspruchsvolle Aufgabe. Es dürfe bei den Regelungen kein Interpretationsspielraum bleiben, denn einheitliches Recht brauche einheitliche Anwendung. Aufgrund Europas weltweiter Vorbildwirkung in der Rechtssetzung braucht Datenschutz in einer globalisierten Welt außerdem einen hohen, international vergleichbaren Standard. Die Haltung des gegenwärtigen deutschen Datenschutzstandards sei für ihn ein „Minimalziel". Das „Recht auf Vergessen" bezeichnete er als einen eigentlich gar nicht so neuen „Löschungsanspruch 2.0", der die modernen Entwicklungen beispielsweise bei den Social Media aufgreife. Die Verordnung müsse aber nicht nur unternehmensfreundlich, sondern auch „verbrauchertauglich" sein. Dafür brauche es Informationspflichten, Auskunftsrechte und entsprechende Durchsetzungsmöglichkeiten. Auch er plädierte statt für eine Mitarbeiterzahl als Quorum für Datenschutzbeauftragte für eine intelligentere Lösung.

Die Deutsche Vereinigung für Datenschutz e.V. (DVD) nutzte diese Gelegenheit, um vor allem die praktischen Umsetzungsfragen zu beleuchten: Welche praktischen Auswirkungen werden die vorgesehenen Regelungen der DSGVO haben und welcher Anpassungsbedarf besteht diesbezüglich?

Die Kontrolle über datenschutzgerechtes Handeln ruht auf drei wesentlichen Säulen: der Möglichkeit für Betroffene, individuelle Rechte (Auskunft, Löschung etc.) wahrzunehmen, der innerbetrieblichen Selbstkontrolle (durch Datenschutzbeauftragte, Betriebsräte etc.) und der institutionellen Kontrolle (durch Aufsichtsbehörden und öffentliche Datenschutzbeauftragte). Die DVD hat aufgrund ihrer langjährigen Praxiserfahrung analysiert, mit welchen praktischen Umsetzungsproblemen hierbei zu rechnen wäre. Dabei hat sie in allen drei Bereichen Nachbesserungsbedarf festgestellt und den Abgeordneten erläutert.


Max Schrems, europe-v-facebook.org

Auf der Basis der instruktiven Erfahrungen einer studentischen Initiative aus Österreich berichtete Max Schrems (europe-v-facebook.org) von den praktischen Schwierigkeiten, die auftreten, wenn Bürger ihre Datenschutzrechte in Europa gegen große amerikanische Konzerne durchzusetzen versuchen und dabei auf eine völlig überlastete irische Datenschutzaufsichtsbehörde und einen teuren Rechtsweg angewiesen sind. Selbst die profansten Dinge würden nicht funktionieren, was ihn zu einem Vergleich mit dem Umweltrecht der 60er Jahre veranlasse. Auch damals waren die Forderungen angeblich undurchführbar und viel zu teuer. Eine juristische Klärung zu erreichen, sei im irischen Datenschutzrecht nahezu unmöglich. Vor allem die Kosten gerichtlicher Verfahren machen es aus seiner Erfahrung jedoch zwingend erforderlich, dem Bürger eine kostenfreie, neutrale aber fachkundige Beschwerdeinstanz

zur Seite zu stellen, forderte Schrems die Abgeordneten auf.


Karsten Neumann, DVD

Das Vorstandsmitglied der DVD, Karsten Neumann, beschäftigte sich vor allem mit den Schwierigkeiten in der Rechtsdurchsetzung durch die nationalen Aufsichtsbehörden. Die vorgesehene Untätigkeitsbeschwerde gegenüber Aufsichtsbehörden sei zwar vor dem Hintergrund einiger negativer Erfahrungen verständlich, würde aber die Aufsichtsbehörde selbst zu einem Gegner in einem Rechtsstreit machen und ihre Position schwächen. Besser sei es, den Aufsichtsbehörden den Status eines Betroffenenanwalts oder zumindest eines Sachwalters in gerichtlichen Auseinandersetzungen einzuräumen. Die vorgesehene Verbandsklagemöglichkeit sollte um diesen Punkt ergänzt werden. Anknüpfungspunkt aufsichtsbehördlicher Prüfungen sind in den meisten Fällen Beschwerden von Betroffenen. Diese stützen sich oft auf die Verfahrensverzeichnisse, die nach gegenwärtigem Recht auf Antrag jedermann zugänglich zu machen sind. Diese Regelung ist unverständlicherweise in der DSGVO nicht mehr enthalten und verringert damit die Möglichkeiten öffentlicher Datenschutzkontrolle und der Durchsetzung von Betroffenenrechten. Eine zweite wesentliche Säule aufsichtsbehördlicher Tätigkeit ist die beratende Zusammenarbeit mit den betrieblichen Datenschutzbeauftragten als interne Selbstkontrolle. Vor diesem Hintergrund sind geplante Regelungen, den betrieblichen Datenschutzbeauftragten in die Durchsetzung und Kontrolle der Umsetzung aufsichtsbehördlicher Maßnahmen einzubinden eher bedenklich. Die Aufsichtsbehörden seien auf eine gute Zusammenarbeit mit den betrieblichen Datenschutzbeauftragten ebenso angewiesen, wie diese auf die Möglichkeit vertraulicher Beratung innerhalb des Unternehmens. Schon deshalb dürften die betrieblichen Datenschutzbeauftragten nicht als „Informant“ der Aufsichtsbehörden wahrgenommen werden. Für die vorgesehene Bestellpflicht eines Datenschutzbeauftragten schlug Neumann eine Anknüpfung an die Risikobewertung nach Artikel 33 des Entwurfes vor. Danach ist bei Verarbeitungsvorgängen, die aufgrund ihres Wesens, ihres Umfangs oder ihrer Zwecke konkrete Risiken für die Rechte und Freiheiten betroffener Personen bergen, vorab eine Technikfolgenabschätzung der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten durchzuführen. Unternehmen, die eine solchen Risikobewertung durchführen müssen, sollten unabhängig von der Mitarbeiterzahl einen Datenschutzbeauftragten bestellen(siehe ausführlich DANA 2/2012).


Karin Schuler, DVD

Aus der Sicht betrieblicher Praxis betonte Karin Schuler, Vorsitzende der DVD, die Notwendigkeit einer europaweit einheitlichen und verbindlichen Regelung. Bei aller Kritik an Einzelpunkten sei zu beachten, dass es keine nationalstaatliche Alternative hierzu gibt. Die Verordnung müsse vor allem strengere Sanktionen enthalten, die Unternehmen nicht mehr „aus der Portokasse“ bezahlen könnten, um wirkliche Umsetzung zu ermöglichen. Kostenlos sei Datenschutz nicht zu haben. Die Probleme zunehmender internationaler Vernetzung habe der Entwurf noch nicht wirklich erfasst. Der neu eingeführte Begriff der Unternehmensgruppe führe hier eher zu Verwirrung. Besonders prekär seien die immer noch fehlenden klaren gesetzlichen Vorgaben zur personellen und sachlichen Ausstattung der Datenschutzbeauftragten. Hier sei noch zu oft die Bestellung nur ein Feigenblatt, ohne dass der Bestellte konkrete Umsetzungsmöglichkeiten für Datenschutz im Unternehmen hätte. Auch eine Berufsgeheimnisträgerregelung sei noch erforderlich, um die Position der Datenschutzbeauftragten zu stärken. Die Arbeitnehmervertretungen als ein Akteur im betrieblichen Datenschutz fehlten bisher völlig. Auch wenn es sich hier um ein spezifisch deutsches Problem handeln sollte, so wären die Folgen beispielsweise in der Ermächtigungsnorm für die Nationalstaaten zum Thema Beschäftigtendatenschutz in Artikel 82 zu regeln. Hier fehle gegenwärtig eine Befugnis, durch Gesetz auch Betriebsvereinbarungen als Rechtsgrundlage für Datenverarbeitungen zuzulassen, ergänzte der souveräne Moderator der Matinée, Sönke Hilbrans, stellvertretender Vorsitzender der DVD, die Ausführungen und dankte im Namen der DVD den Abgeordneten und insbesondere der Einladerin Frau Birgit Sippel für die erneute Gastfreundschaft in Brüssel. Frau Sippel ihrerseits dankte für die Anregungen aus dieser Veranstaltung und forderte die DVD auf, sich auch weiterhin mit Anregungen an dem Diskussionsprozess zu beteiligen.


Sönke Hilbrans, DVD



Datenschutz im Meldewesen stärken, nicht schwächen!

Egal ob E-Mail-Adresse oder Postanschrift: Wer seine Daten allzu leichtfertig heraus gibt, wird schnell mit unerwünschter Post bombardiert. Daher sind viele Menschen vorsichtig, wenn es um die Herausgabe persönlicher Daten geht. Doch an einer Stelle ist man dazu verpflichtet: Jede/r Bürger/in muss sich mit seinem/ihrem Wohnsitz beim örtlichen Einwohnermeldeamt melden.

Für Adresshändler und die Werbe-Industrie sind diese Datenbanken der Meldebehörden ein Schatz - und eine Neuregelung des Melderechts hat ihnen den Weg zu dieser Goldgrube jetzt noch leichter gemacht. Künftig sollen die Meldeämter Adressdaten an Werbetreibende oder Adresshändler verkaufen dürfen – ohne dass man dies verhindern kann.

Doch noch ist das Gesetz zum Glück nicht in Kraft: Erst müssen die Bundesländer im Bundesrat mehrheitlich zustimmen. Bislang haben sie sich dazu noch nicht positioniert. Mit einem Online-Appell fordern wir die Ministerpräsident/innen der Länder auf, die Regelung im Bundesrat zu Fall zu bringen.

Die Neuregelung des Melderechts

Seit der Föderalismusreform 2006 hat der Bund die ausschließliche Gesetzgebungskompetenz für das Meldewesen. Das alte Melderechtsrahmengesetz stammte von 1980 und musste daher dringend überarbeitet werden. In dem Gesetz wird geregelt, wie die Einwohnermeldeämter mit den Daten der bei ihnen gemeldeten Bürger/innen umgehen dürfen bzw. müssen. Ursprünglich wollte das Innenministerium ein zentrales Melderegister einrichten. Dieser Plan wurde jedoch 2008 unter dem Eindruck etlicher Datenskandale auf Eis gelegt.

Ende November 2011 legte das Innenministerium dann einen Entwurf für ein „Gesetz zur Fortentwicklung des Meldewesens“ vor. Der Entwurf sah noch eine Stärkung der Rechte der Bürgerinnen und Bürger vor: Im Artikel 44, der die „einfache Melderegisterauskunft“ regelt, war vorgesehen, dass Meldebehörden Daten an Werbetreibende oder Adresshändler nur dann weitergeben dürfen, wenn die betreffende Person dem vorher aktiv zugestimmt hat.

Datenweitergabe als Standard

Wenige Tage vor der endgültigen Abstimmung im Bundestag setzten CDU- und FDP-Politiker/innen im Innenausschuss jedoch Änderungen durch, die diese Regelung zum Schutz unserer Daten ins genaue Gegenteil verkehren: Daten sollen jetzt grundsätzlich herausgegeben werden dürfen – auch zur Zwecke der Werbung und des Adresshandels. Will man dies verhindern, muss man dagegen ausdrücklich Widerspruch einlegen. Die Weitergabe persönlicher Daten wird damit von der Ausnahme zum Standard – und unsere Daten werden zur freien Ware für die Adress- und Werbe-Wirtschaft.

Widerspruch zwecklos: Goldgrube für Datenhändler

Doch der Skandal geht noch weiter: Selbst dieser Widerspruch bleibt in den meisten Fällen nichtig. Denn in dem neuen Paragraphen ist außerdem festgeschrieben, dass der Widerspruch nicht gilt, „wenn die Daten ausschließlich zur Bestätigung oder Berichtigung bereits vorhandener Daten verwendet werden.“ Da man für eine Melderegisterauskunft stets bereits vorhandene Daten benötigt, gilt der Widerspruch praktisch nie. Damit wird der Datenschutz in Meldebehörden faktisch abgeschafft.

Für die Adresshändler ist diese Regelung Gold wert: Mit der Neuregelung werden die Einwohnermeldeämter zum Selbstbedienungsladen. Wieder einmal haben Lobbyisten von Adressfirmen und Auskunfteien (private Daten-Auskunfts-Firmen, wie etwa die SCHUFA) dafür gesorgt, dass eine geplante datenschutzfreundliche Regelung in ihr Gegenteil verkehrt wurde.



Bild: Campact

Gegen die Adress-Lobby – für mehr Datenschutz!

Gegen diese Auflösung des Datenschutzes zugunsten der Adress- und Datenlobby müssen wir uns wehren! Dieses Gesetz darf so nicht beschlossen werden. Denn es widerspricht dem Grundgesetz, das uns das Recht zusichert, selbst zu entscheiden, was mit den eigenen Daten geschieht.

Voraussichtlich im September entscheidet der Bundesrat über das Gesetz. Bis dahin wollen wir - gemeinsam mit unseren Kooperationspartnern FoeBuD e.V. und dem Verbraucherzentrale Bundesverband (vzbv) und der Vereinigung für Datenschutz - mindestens 100.000 Unterschriften sammeln und sie den Ministerpräsident/innen überreichen. FoeBuD e.V. setzt sich seit 25 Jahren für Datenschutz und Bürgerrechte ein und richtet die jährlichen Big-Brother-Awards aus, einen Negativpreis für Unternehmen, Institutionen und Einzelpersonen, die besonders eklatant die Privatsphäre von Menschen beeinträchtigen oder persönliche Daten Dritten zugänglich machen.

Quelle: https://www.campact.de/melderecht/appell/5-minuten-info/

Ein Gesetz in nur 57 Sekunden...



„...den Tagesordnungspunkt 21, zweite und dritte Beratung des von der Bundesregierung eingebrachten Gesetzentwurfs zur Fortentwicklung des Meldewesens."



„Wie in der Tagesordnung ausgewiesen, werden die Reden zu Protokoll genommen und wir kommen zur Abstimmung."



„Der Innenausschuss empfiehlt in seiner Beschlussempfehlung auf Drucksache 10158 den Gesetzentwurf der Bundesregierung auf Drucksachen 7746 in der Ausschussfassung anzunehmen."



„Ich bitte diejenigen, die zustimmen wollen, um das Handzeichen. Danke."



„Wer stimmt dagegen? Danke. Wer enthält sich? Der Gesetzentwurf ist damit in zweiter Beratung angenommen."



„Dritte Beratung und Schlussabstimmung. Ich bitte diejenigen, die dem Gesetzentwurf zustimmen wollen, sich zu erheben. Danke."



„Wer stimmt dagegen? Danke. Wer enthält sich? Der Gesetzentwurf ist angenommen."









Gemeinsame Pressemitteilung

Meldegesetz: 190.000 Unterschriften an Bundesländer überreicht

Übergabe von 190.000 Unterschriften gegen Meldegesetz an Innenministerien der Bundesländer / Bürger fordern Einwilligungsregelung / „Ohne Einwilligung dürfen Meldeämter keine Daten an Adresshändler oder Werbetreibende weitergeben“

Berlin, 6.9.2012. Vor der Sitzung des Bundesrats-Innenausschusses übergab das Bündnis „Meine Daten sind keine Ware“ mehr als 190.000 Unterschriften gegen das neue Meldegesetz an die Innenministerien der Bundesländer. Die Unterzeichner fordern von den Ländern, die Weitergabe von Meldedaten an Adresshändler und Werbetreibende künftig nur mit ausdrücklicher Einwilligung der Bürger zu erlauben. Symbolisch verschlossen Bündnisvertreter bei der Unterschriftenübergabe „Meldeakten“ mit stabilen Vorhängeschlössern.

Das Bündnis kritisiert, dass Bürgerinnen und Bürger mit dem Gesetz des Bundestags keine Möglichkeit mehr hätten, sich gegen die Weitergabe ihrer Daten zu wehren. Der Bundestag hatte die ursprünglich vorgesehene Einwilligungslösung ("Opt-In") in der aktuellen Gesetzesfassung zugunsten eines nachträglichen Widerspruchsrechts ("Opt-Out") abgeschafft. Durch eine Zusatzklausel wird jedoch selbst dieses Widerspruchsrecht faktisch ausgehebelt. "Jetzt muss der Bundesrat das Gesetz stoppen – und für mehr Datenschutz sorgen“, so Karsten Neumann von der Deutschen Vereinigung für Datenschutz.

„Beim Melderecht darf es jetzt keine faulen Kompromisse geben: Ohne Einwilligung der Bürgerinnen und Bürger dürfen Meldeämter keine Daten an Adresshändler oder Werbetreibende verkaufen“, forderte Christoph Bautz vom Kampagnennetzwerk Campact.

Rena Tangens vom Bürgerrechts- und Datenschutzverein FoeBuD stellte klar: „Meldebehörden sind kein Selbstbedienungsladen für Adresshändler. Datenschutz im Meldeamt muss die Regel und nicht die Ausnahme sein.“

„Datenschutz darf für Behörden keine Fußnote sein. Da Bürger verpflichtet sind, ihre Daten bei Meldebehörden anzugeben, müssen sie aktiv um Einwilligung gebeten werden, bevor ihre Daten weiter gegeben werden“, erklärte Gerd Billen, Vorstand des Verbraucherzentrale Bundesverbands (vzbv).

Das Bündnis wird getragen vom Kampagnennetzwerk Campact, dem Bürgerrechts- und Datenschutzverein FoeBuD e.V., dem Verbraucherzentrale Bundesverband und der Deutschen Vereinigung für Datenschutz. Der Online-Appell der Kampagne findet sich unter https://www.campact.de/melderecht/appell/.

Datenschutznachrichten

Datenschutznachrichten aus Deutschland

Bund

Hasso-Plattner-Institut kündigt Forschungsauftrag der Schufa

Deutschlands größte Auskunftei, die „Schutzgemeinschaft für allgemeine Kreditsicherung“ – kurz Schufa, plante, in sozialen Netzwerken wie Facebook und aus zahlreichen anderen Quellen im Internet gezielt Daten über VerbraucherInnen zu sammeln. Das Wiesbadener Unternehmen ließ hierfür am Hasso-Plattner-Institut der Universität Potsdam (HPI) entsprechende Projektvorschläge entwickeln. Demgemäß sollten unter anderem die Kontakte von Facebook-Mitgliedern herangezogen werden, um Beziehungen zwischen Personen zu untersuchen und so Zusammenhänge mit der Kreditwürdigkeit der VerbraucherInnen zu finden. Die Analyse von Textdaten wurde angedacht, um „ein aktuelles Meinungsbild zu einer Person zu ermitteln.“ Die WissenschaftlerInnen sollten untersuchen, wie die Schufa über eigene Facebook-Profile oder Zugänge zum Kurznachrichtendienst Twitter verdeckt an „Adressen und insbesondere Adressänderungen“ anderer Nutzenden gelangen kann. Angedacht war auch die „automatisierte Identifikation von Personen öffentlichen Interesses, Verbraucherschützern und Journalisten“.

In dem Projektpapier hieß es weiter: Mit den Daten „soll ein Pool entstehen, der von der Schufa für existierende und künftige Produkte und Services eingesetzt werden kann.“ Allgemein gehe es darum, „Chancen und Bedrohungen für das Unternehmen zu identifizieren und zu bewerten.“ In den Dokumenten werden neben Facebook auch berufliche Netzwerke wie Xing oder LinkedIn, Personensuchmaschinen wie Yasni, Geodatendienste wie Google Streetview sowie MitarbeiterInnenverzeichnisse von Unternehmen aufgeführt, aus denen Daten gewonnen werden könnten. Solche Informationen könnten schließlich mit Schufa-eigenen Verbraucherdaten verknüpft werden, um sie „aus Business-Sicht zu bewerten.“ Vorgesehen war, dass die Schufa dem Institut 200.000 Euro pro Jahr bezahlt.

Vertreter der Schufa und des HPI bestätigten die Recherchen von NDR Info. Das Institut hatte zum 01.04.2012 ein Forschungsprojekt mit dem Namen „Schufa-Lab@HPI“ eingerichtet. Die in Presseberichten zitierte Sammlung von Projektideen sei „in Gesprächen zwischen dem HPI-Fachgebiet Informationssysteme und dem Projektpartner Schufa entstanden.“ Es handele sich dabei lediglich um „Grundlagenforschung“, die man nach „höchsten ethischen Maßstäben“ betreibe. Schufa-Vorstand Peter Villa betonte, dass sein Unternehmen sich „durch wissenschaftlich fundierte Ergebnisse langfristig die Qualitätsführerschaft unter den Auskunfteien in Deutschland sichern“ wolle.

Daten- und Verbraucherschützer reagierten auf die Schufa-Pläne mit Entsetzen und Unverständnis. Der schleswig-holsteinische Landesdatenschutzbeauftragte Thilo Weichert sagte: „Hinter einem solchen Forschungsprojekt steckt immer eine Absicht. Sollte die Schufa die gewonnenen Daten tatsächlich einsetzen, wäre das eine völlig neue Dimension.“ Er zweifle daran, dass eine Umsetzung der Projektideen rechtlich haltbar sei. Edda Castelló von der Verbraucherzentrale Hamburg nannte das Schufa-Projekt eine „Grenzüberschreitung“. „Wenn diese sehr privaten und persönlichen Datensammlungen wie Facebook von der Schufa zusammengeführt und ausgenutzt werden, dann wird es hochgefährlich.“

Die Veröffentlichung über das Projekt führte zu massiver öffentlicher Kritik. Verbraucherschutzministerin Ilse Aigner (CSU) bezeichnete das Vorhaben eine Schnapsidee: „Wenn sogar in dem geschlossenen Bereich versucht wird, Daten zu ermitteln, ist das schon ein massiver Eingriff. Aber generell kann man den Verbrauchern nur raten, sparsam mit den Daten umzugehen.“ Ähnlich äußerte sich auch Bundesjustizministerin Sabine Leutheusser-Schnarrenberger (FDP): „Es darf nicht sein, dass Facebook-Freunde und Vorlieben dazu führen, dass man zum Beispiel keinen Handyvertrag abschließen kann. Welche Daten dazu führen, ob jemand als zahlungsfähig eingestuft wird, ist jetzt schon umstritten.“ FDP-Bundestagsfraktionschef Rainer Brüderle forderte die Schufa auf, von ihren Plänen „Abstand zu nehmen“. Für die SPD sprach der Vize-Vorsitzende der Bundestagsfratkion Ulrich Kerber von einem „Horrorszenario“. Grünen-Fraktionschefin Renate Künast sprach von einem „offenkundig verfassungswidrigen Vorhaben“. Der netzpolitische Sprecher der Grünen-Bundestagsfraktion Konstantin von Notz warnte: „Arbeitgeber werden Mitarbeiter überprüfen wollen, Geheimdienste nach verdächtigem Verhalten suchen. Die Bundesregierung muss endlich das Datenschutzrecht reformieren und Unternehmen in ihre Schranken weisen.“ Bernd Schlömer, Vorsitzender der Piratenpartei, meinte, die Berichte über die geplante Datensammlung hätten auch ihr Gutes. Sie verdeutlichten, wie sensibel persönliche Daten im Internet sind: „An den Schufa-Aktivitäten kann man sehen, dass gegebenenfalls leichtfertig bereit gestellte persönliche Daten von Dritten genutzt werden für Auswertungsprofile.“

Auch der Branchenverband Bitkom reagierte deutlich: Nicht alles, was technisch machbar sei, dürfe auch umgesetzt

werden. Wer soziale Netzwerke durchforste, verunsichere die Verbraucher, meinte Bitkom-Präsident Dieter Kempf. Es wäre klug, auf solche Gedankenspiele zu verzichten.

Der Berliner Datenbank-Spezialist und Blogger Christian Köhntopp wies darauf hin, dass die Planungen der Schufa schon Praxis einiger Unternehmen ist, in jedem Fall bei der Vermarktung von gezielter Werbung oder auch bei der Suche nach neuen Mitarbeitern. Dieselben Nutzenden, die sich nun über die Schufa aufregen, vertrauten zuvor freizügig ihre intimsten Daten den Servern der diversen kostenlosen sozialen Netzwerke an. Wer für einen Service nicht zahlen müsse, werde selbst zum Produkt, warnte der Bundesdatenschutzbeauftragte, Peter Schaar: „Der Fall zeigt einmal mehr, wie Nutzerdaten – etwa aus sozialen Netzwerken wie Facebook – ohne Wissen der Betroffenen ausgeforscht und zu Geld gemacht werden.“ Constanze Kurz, Sprecherin des Chaos Computer Clubs, kommentierte: „Wir sind das Produkt. Wir sind das Schaf, das geschoren wird. Studien haben ergeben, dass über 76% bei ihren Profilen im Internet nicht lügen oder auch nur beschönigen.“

Big Data heißt dieser Mega-Trend im Netz. Vorreiter bei der intelligenten Verknüpfung von Nutzer-Informationen war der kalifornische Suchmaschinengigant Google. Dann baute der Freeware-Progammierer Doug Cutting 2005 die Google-Software nach und stellte sie unter dem Namen „Hadoop“ in freier Lizenz umsonst zur Verfügung. Inzwischen läuft Hadoop auf Millionen Servern weltweit. Aus mit Positionsdaten versehenen Urlaubsfotos von Facebook lässt sich herauslesen, wer wann wo in den Urlaub fährt. Daraus wiederum sind Rückschlüsse auf die Einkommenssituation und persönliche Freizeitpräferenzen der Nutzer möglich – Daten, die nicht nur die Schufa interessieren könnten, sondern auch Reiseportale oder Outdoorhersteller. Auf dem Karriereportal Xing lassen sich einfach Zusammenhänge zwischen dem beruflichen Erfolg und dem Uni-Abschluss erkennen – spannend für Personalberater, die Absolventen einer bestimmten Hochschule bevorzugen könnten. Wer seine Daten im Netzwerk gegen solche Analysen mit Privacy-Einstellungen schützt, kann bei der Kreditberatung oder im Vorstellungsgespräch zur Freigabe des eigenen Nutzerkontos aufgefordert werden (siehe S. 128). In den USA werden beim Anbieter Identified Daten aus sozialen Netzwerken für Ratings bei der Arbeitsplatzsuche genutzt (DANA 1/2012, 34f) oder für generell im Geschäftsbereich einsetzbare Scorings. Der IT-Forensikprofessor an der Hochschule der Polizei in Hamburg Tobias Eggendorfer wunderte sich nicht über das Interesse der Schufa und anderer Firmen an den Daten aus sozialen Netzwerken: „Steht auf meiner Facebook-Seite, dass ich gern Fallschirmspringen gehe, würde meine Berufsunfähigkeitsversicherung mich vielleicht als Risikosportler einstufen. Poste ich, dass ich ein extremer Autofahrer bin, glaubt vielleicht mein Autohändler nicht mehr, dass der Verschleiß meiner Bremsen auf einem Materialfehler beruht.“

In Reaktion auf die Kritik äußerten sich sowohl das Hasso-Plattner-Institut als auch die Schufa. Es handele sich hier nur um Grundlagenforschung; man wolle einen Diskurs anregen. Alles geschehe im Rahmen des Gesetzes. Ihren eigenen Verbraucherbeirat hat die Schufa von dem Projekt nichts erzählt - mehrere Mitglieder des Gremiums beschwerten sich deshalb bei Schufa-Chef Michael Freytag. Bei Twitter dagegen liefen derweil ständig neue Ideen ein, der Schufa ein Schnippchen zu schlagen, vorgespielter Reichtum gegen schlechtes Scoring liest sich dort zum Beispiel so: „James, der Champagner im Bentley war heute etwas zu warm.“

Zwei Tage nach der ersten Veröffentlichung und vernichtender Kritik kündigte das Hasso-Plattner-Institut (HPI) die Zusammenarbeit mit der Schufa. Das Projekt sei in der Öffentlichkeit auf Missverständnisse gestoßen. Daher könne es „nicht unbelastet und mit der nötigen Ruhe durchgeführt werden“, erklärte HPI-Direktor Christoph Meinel. Ein Twitter-Kommentar: „Mist, der Ferrari hat ´nen Platten. Jetzt müssen wir wieder mit dem Q7 nach Sylt.“

In den USA ist man hinsichtlich der Auswertung von Internetdaten für Zwecke der Bewertung der Kreditwürdigkeit schon weiter als in Deutschland. Ken Lin, CEO beim bankenunabhängigen Kreditdienstleister Credit Karma, beschreibt, was heute schon so alles an Verwertbarem über die Kundschaft aus dem Netz gefischt wird und auf welche künftigen Erkenntnisinteressen sich die NetzbürgerInnen schon mal einstellen können: „Vielen US-Bürgern wird es nicht bewusst sein, dass ihre Social-Media-Konversationen Banken und anderen Kreditoren sehr wertvolle Informationen liefern.“ Diese Informationen würden in großen Datenbanken gesammelt und analysiert, um Kreditgebern Entscheidungshilfen sowohl im Marketing als auch in der Bonitätsbewertung zu liefern. Gesucht werde nach allem, was auf eine Änderung der finanziellen Verhältnisse schließen lässt (also Informationen wie Jobwechsel, Arbeitsplatzverlust etc.), wie es um das Social-Media-Umfeld finanziell bestellt ist und ob sich generell größere Umbrüche in der Lebenssituation andeuten, die zum Beispiel auf Heirat/Familiengründung und Ähnliches hinweisen (www.ndr.de 07.06.2012 u. 08.06.2012; Fuest/Ehrenstein www.welt.de 07.06.2012; www.zeit.de 07.06.2012; Heinrich/Kolenberg KN 08.06.2012, 3; KN 09.06.2012, 9; Fromm SZ 09./10.06.2012, 28; Der Spiegel 24/2012, 75; Settembrini di Novertre www.faz.net 21.06.2012).

Bund

Generalbundesanwalt schlägt elektronische Fußfessel für Hooligans vor

Generalbundesanwalt Harald Range schlug in einem Zeitungsinterview elektronische Fußfesseln für „notorische Hooligans“ vor, um die schon bestehenden Stadionverbote besser umsetzen zu können. Nach der derzeitiger Rechtslage sei dies unmöglich. Der Vorsitzende der Innenministerkonferenz und Innenminister von Mecklenburg-Vorpommern, Lorenz Caffier (CDU), forderte zeitgleich, die Einlasskontrollen bei Fußballspielen zu verstärken und personalisierte Eintrittskarten einzu-

führen. Anlass waren finstere Szenen, als z. B. Fußballfans schon vor Abpfiff des Relegationsspiels zwischen Fortuna Düsseldorf und Hertha BSC am 15.05.2012 den Rasen stürmten und Dutzende bengalischer Fackeln entzündeten. Bundesinnenminister Hans-Peter Friedrich (CSU) verlangte dagegen nur, die bestehenden Mittel müssten besser genutzt werden und alle Verantwortlichen „an einem Strang ziehen".

Volker Goll von der Koordinationsstelle der Fanprojekte bezeichnete diese Diskussion einen „Wettbewerb der Stammtischparolen". Es werde der falsche Eindruck erweckt, es gäbe ein Gewaltproblem, das mit normalen strafrechtlichen Mitteln nicht zu lösen sei. Offenbar solle für Fußballfans eine Art „Ersatzstrafrecht" gelten. Er kritisierte die bundesweiten Stadionverbote, die nun mit Fußfesseln durchgesetzt werden sollen. Die Verbote würden die Vereine auf Anregung der Polizei aussprechen, wenn diese Ermittlungen gegen einzelne Fans einleitet. Goll plädiert stattdessen dafür, dass die Fußballvereine ihr Hausrecht nutzen sollten. Sie könnten die verdächtigen Fans anhören und danach als „Warnschuss" ein Hausverbot erteilen. Im Jahr 2011 erhielten weniger Fußballfans bundesweite Stadionverbote als zuvor. Waren in der Saison 2009/2010 knapp 3.800 Stadionverbote in Kraft, so sank deren Zahl laut Jahresbericht der Zentralen Informationsstelle für Sporteinsätze am Ende der folgenden Saison auf etwa 2.500 (Janke SZ 26.-28.05.2012, 8, auch S. 2).

Bund

Familienministerium plant vertrauliche Geburt

Die Daten von Müttern, die bei der Geburt ihres Kindes ihre eigene Identität nicht preisgeben wollen, sollen künftig 16 Jahre unter Verschluss gehalten werden. Danach soll das Kind ein Recht darauf haben, seine Abstammung zu erfahren. Das geht aus einem Eckpunktepapier des Familienministeriums zur «vertraulichen Geburt» hervor. Man habe damit eine ausgewogene Regelung gefunden, die den Wunsch der Mutter nach Anonymität respektiere und dem Recht des Kindes auf eine eigene Identität nachkomme, sagte Familienministerin Kristina Schröder. Ein nach diesen Prinzipien erarbeitetes Gesetz soll vor allem Babyklappen überflüssig machen. Diese sind derzeit - wie auch anonyme Geburten - rechtlich unzulässig und werden lediglich geduldet (SZ 05.07.2012, 6; www.stern.de 04.07.2012)

Bundesweit

Wildkameras erfassen auch Menschen

PolitikerInnen und DatenschützerInnen sehen sich mit einem neuen „Datenschutzproblem" konfrontiert: den Wildkameras. Deren Zweck ist es, seltene Lebewesen im Wald zu erfassen und im Blick zu behalten. So wurden Anfang Juni 2012 zwei Wölfe in der Lüneburger Heide gesichtet. Auch Jäger stellen gut getarnte Kameras auf, um einen besseren Überblick über den Wildwechsel zu erhalten. Doch erweist sich, dass immer wieder Menschen in die Foto- und Videofallen tappen. In Kärnten wurde ein Fall publik, bei dem das außereheliche Schäferstündchen eines Politikers im Wald abgelichtet wurde. Der Leiter des Bayerischen Landesamtes für Datenschutzaufsicht Thomas Kranig zieht seine Konsequenzen: „Wenn die Kameras personenbezogene Daten aufnehmen, dann ist dies rechtswidrig." Ein mögliches öffentliches Interesse, etwa wenn Jäger Wildbestände dokumentieren wollen, werde von seiner Behörde „sehr restriktiv ausgelegt". Die Opfer der Fotofallen merken selten etwas von den Aufnahmen. Die Geräte verfügen über Infrarotblitze, die für Mensch und Tier unsichtbar sind. Werden Bilder an den Verantwortlichen übertragen, so müsste diese die Aufnahmen von Menschen unverzüglich löschen. Aldi Süd bietet ab Ende Juni 2012 eine Wildkamera zu einem Niedrigpreis an, laut Werbung „optimal geeignet zur Überwachung von Tieren, Grundstücken, Gebäuden oder anderen schwer einsehbaren Orten". Die bayerische SPD forderte Klarheit, ob die Geräte im öffentlichen Bereich überhaupt eingesetzt werden dürfen (Der Spiegel 26/2012, 16).

Bundesweit

Kameras sollen TaxifahrerInnen schützen

TaxikundInnen können in Bälde in Frankfurt und in manchen anderen Orten verwundert feststellen, dass - kaum eingestiegen - ihr Bild auf einem Display am Armaturenbrett aufleuchtet. Das Porträt und weitere Aufnahmen des Fahrgastes während der Fahrt werden für 24 Stunden gespeichert. Das allererste Bild, so die Vorstellungen von Hans-Peter Kratz, Chef der Taxivereinigung Frankfurt, soll an die Taxi-Zentrale weitergeleitet werden. Die Aufnahmen sind Kern eines neuen Sicherheitskonzepts, mit dem böse Menschen von bösen Taten in den Taxis abgehalten werden sollen. In Bremen hat die Im-Auto-Kamera die Zahl der Übergriffe auf Taxifahrer und die Auseinandersetzungen zwischen Dienstleister und Fahrgästen signifikant sinken lassen, seit dort seit Sommer 2011 TaxikundInnen „geblitzt" werden. Die Bremer Datenschutzbeauftragte, so Kratz, habe mit bestimmten Auflagen grünes Licht gegeben. „Die Resonanz ist durchweg positiv." Nach Kontaktaufnahme mit dem Hessischen Datenschutzbeauftragten sei man sich einig, dass die Bilder verpixelt oder anderweitig verschlüsselt und nach 24 Stunden gelöscht werden, falls die Beförderung ohne Zwischenfälle verlaufen ist. Falls es Probleme gegeben hat, sollen nach dem Vier-Augen-Prinzip Polizei oder Ordnungsbehörde gemeinsam mit einem Vertreter der Taxi-Seite die Bilder entschlüsseln und damit den Fahrgast enttarnen. Die Kameras sollen der Abschreckung dienen, so Kratz, „damit potenzielle Straftäter die Finger von uns lassen". In Bremen machen die Kameras alle 15 Sekunden ein Foto. Wenn es nach dem Frankfurter Taxi-Chef ginge, dann würden die Insassen während der gesamten Fahrt gefilmt „und Ton sollte meiner Ansicht nach auch aufgezeichnet werden." Kratz verspricht sich von der Rundum-Überwachung auch die Klärung strittiger Situationen. Oft würde über die richtige Fahrtstrecke und die Gebühren gestritten. Der Taxi-Unternehmer glaubt, das könnte auch im Interesse der Fahrgäste sein. Der Hessische Datenschutzbeauftragte signa-

lisierte jedoch, dass Ton gar nicht gehe. Die Taxivereinigung lässt momentan außerhalb des normalen Fahrbetriebes mehrere Kamera- und Aufzeichnungssysteme auf ihre Alltagstauglichkeit hin prüfen. Der Einbau soll pro Taxi 800 bis 1000 Euro kosten: „Das sollte uns Leib und Leben unserer Taxifahrer wert sein" (Ahäuser wwww.fr-online.de 25.06.2012; vgl. ULD, https://www.datenschutzzentrum.de/video/20120112-videoueberwachung-taxis.html, 11.01.2012).

Bayern

Datenschutzbeauftragter legt Prüfbericht zu Staatstrojaner vor

Der bayerische Datenschutzbeauftragte Thomas Petri hat gemäß einem veröffentlichten Prüfbericht zur Nutzung der Quellen-TKÜ (Telekommunikationsüberwachung) durch bayerische Behörden Datenschutzverstöße festgestellt, die sich „im tiefdunklen Graubereich" bewegen. Das Land Bayern nutzte ausschließlich Software der hessischen Firma Digitask. Zuvor hatte schon der Bundesdatenschutzbeauftragte festgestellt, dass auch bei Bundesbehörden gravierende Fehler gemacht wurden und die Quellen-TKÜ mangelhaft ist.

Die bayerischen Strafverfolgungsbehörden haben im Zeitraum von 2008 bis 2011 in 23 Fällen nach richterlicher Anordnung eine Quellen-TKÜ mit Trojaner-Software durchgeführt. Petri war tätig geworden, nachdem der Chaos Computer Club den bayerischen Staatstrojaner 0zapftis enttarnt und seine Funktionsweise entschlüsselt hatte. Petri bemängelte, dass die TKÜ-Aktionen unvollständig dokumentiert wurden. Die Abläufe seien nicht nachvollziehbar. Die von Digitask gelieferte Software sei fehlerhaft gewesen, da sie in 4 von 20 Fällen Browser-Screenshots ermöglichte, was nicht richterlich angeordnet gewesen sei. In 2 weiteren Fällen waren bei Testinstallationen der Datenschützer verbotene Screenshots des gesamten Bildschirms möglich. In 9 von 20 Fällen hätten die Behörden komplette Softwarelisten der belauschten Rechner ausgelesen und gespeichert, ohne dass dies angeordnet worden sei. Die Softwarelisten auszulesen sei dabei besonders bedenklich, da dabei eine Quellen-TKÜ nicht von einer verbotenen Onlinedurchsuchung unterschieden wird. Die bayerischen Datenschützer bemängelten, die Strafverfolger hätten nicht den Quellcode einsehen können. Höchst bedenklich sei, dass das private Wartungspersonal der Firma Digitask nicht auf das Datengeheimnis nach dem Verpflichtungsgesetz hingewiesen wurde. Es wurden ausländische Server zur TKÜ-Ausleitung benutzt, die fremdstaatlichen Rechten unterliegen. Die dabei eingesetzte Verschlüsselung sei für die Jahre 2008 bis 2010 ausreichend, heute aber technisch unzureichend. Über den gesamten Zeitraum hinweg sei die Überwachungskonsole nicht mit Updates versorgt und die Nutzung nicht protokolliert worden.

Die Betroffenen waren nach Beendigung der Quellen-TKÜ nicht ausreichend über die „Integritätsbeeinträchtigung" ihrer Rechner informiert worden. In einigen Fällen wurde die Quellen-TKÜ einfach abgeschaltet, der aufgespielte Trojaner aber nicht entfernt. In anderen Fällen, bei denen nach Angaben der Strafverfolger eine Deinstallation erfolgte, konnten die Datenschützer mangels Zugriff auf die Rechner nicht feststellen, wie gut dieser Schritt gelöst wurde. Petris Bericht beschäftigt sich ausführlich mit 9 Fällen bayerischer Staatsanwaltschaften, in denen es hauptsächlich um die Ausleitung von VoIP-Gesprächen via Skype ging. Die Quellen-TKÜ sei ein Verfahren, das erst am Anfang seiner Zweckmäßigkeit stehe und verbessert werden müsse. Die verwendete Software habe mithilfe ihrer Nachladefunktion in großem Umfang unzulässige Datenerhebungen ermöglicht, es lägen aber keine Anhaltspunkte vor, dass Ermittler die Möglichkeiten zum Zugriff auf die gesamten Datensätze auf dem Rechner ausgenutzt hätten. Innenminister Joachim Herrmann (CSU) folgerte daraus, dass sämtliche Vorwürfe gegen seine BeamtInnen „völlig aus der Luft gegriffen" seien.

Er reagierte auf den Prüfbericht mit der Aussage, Bayern werde auch künftig mit Trojanern E-Mails, Chats und Internettelefonate von möglichen Kriminellen ausspionieren. Die Programme seien unverzichtbar und ihr Einsatz rechtlich unproblematisch. Petris Kritikpunkte würden bis zum Herbst 2012 geprüft. Dann solle ein neuer Trojaner einsatzfähig sein. Die alte Software sein inzwischen in technischen Details öffentlich und damit „verbrannt".

Petri stellte hinsichtlich des Regelungsbedarfs folgende Forderungen auf:

„- Sofern Begleitmaßnahmen (z. B. das Auslesen von Softwarelisten zur Vorbereitung der Installation der Software) als notwendig angesehen werden, müssen auch die Art und Weise ihrer Durchführung gesetzlich eindeutig geregelt werden.

- Die Quellen-TKÜ ist durch klare Vorgaben von der Online-Durchsuchung abzugrenzen. Hierbei ist insbesondere die Problematik der Überwachung von Texten außerhalb einer laufenden Telekommunikation zu klären (z. B. Überwachung noch nicht abgesandter E-Mail-Entwürfe).

- Gesetzliche Bestimmungen zur Quellen-TKÜ sind aufgrund ihrer erhöhten Eingriffsintensität in ihren Voraussetzungen enger als die derzeitigen Bestimmungen zur konventionellen Telekommunikationsüberwachung zu fassen.

- Geboten sind weiterhin Regelungen, die technisch und organisatorisch unzulässige Überwachungsfunktionalitäten unterbinden und eine effektive Kontrolle ermöglichen (z. B. Begrenzung von Nachladefunktionen, Möglichkeit einer Einsichtnahme in den Quelltext der Überwachungssoftware).

- Klargestellt werden sollte weiterhin, dass Betroffene nicht nur über die Telekommunikationsüberwachung als solche, sondern auch über den erfolgten Eingriff in ihr IT-System nachträglich zu unterrichten sind" (Borchers www.heise.de 02.08.2012; Hollenstein SZ 03.08.2012, 5; BayLfD PM 02.08.2012).

Berlin

Springer macht aus Datenschutzanfragen Computersabotage

Der Axel Springer Verlag versendete im Rahmen seiner Aktion „Bild für

alle“ im Juni 2012 anlässlich des 60. Geburtstags der Boulevard-Zeitung eine Gratisausgabe an über 40 Millionen deutsche Haushalte. Zahlreiche Gegner der Marketingmaßnahme riefen zum Boykott und zu Gegenaktionen auf. Auch das Polit-Blog netzpolitik.org veröffentlichte unter der Überschrift „Den Springer-Verlag effektiv zurücktrollen“ ein Musterschreiben sowie die Ankündigung des Autors, dieses an acht verschiedene E-Mail-Adressen des Springer Verlags zu übersenden, damit sichergestellt ist, dass das Schreiben auch ankommt. In dem Musterschreiben wird unter anderem eine Auskunft über die bei Springer gespeicherten personenbezogenen Daten des Verfassers gefordert. Der Verlag antwortete per Brief, erteilte jedoch nicht die geforderten Auskünfte. Daraufhin erneuerten der Netzpolitik-Autor Linus Neumann und zahlreiche LeserInnen die entsprechende Anfrage.

Statt den gesetzlichen Vorgaben zu folgen, versandte die Axel Springer AG nunmehr eine Mail an zahlreiche VerfasserInnen der Auskunftsforderungen. Darin wird ausgeführt, dass sich der Verlag hinsichtlich der Anfragen mit der Berliner Datenschutzbehörde abgestimmt habe. Den „Petenten“ wird vorgeworfen, dass es ihnen „nicht auf die datenschutzrechtliche Anfrage, sondern darauf ankam, unsere Kommunikationseinrichtungen zu blockieren“. Ein solches „E-Mail-Bombing“ stelle einen „rechtswidrigen Eingriff in unseren eingerichteten und ausgeübten Gewerbebetrieb dar und erfüllt außerdem den Tatbestand der Computersabotage gem. § 303 b StGB“. Wolle man die datenschutzrechtliche Anfrage aufrecht erhalten, so solle man eine Kopie der Vorder- und Rückseite des Personalausweises übersenden, da man sich „vor der Erteilung der Auskünfte über die Identität des Petenten versichern“ müsse.

Natürlich ist die Argumentation mit dem § 303 b StGB rechtlich nicht zu halten. Fragwürdig ist auch die Aufforderung, eine Kopie des Personalausweises zu übersenden. Bei dem seit 2010 verteilten neuen Ausweis darf eine Kopie nur für die im Personalausweisgesetz genannten Zwecke angefertigt werden. Die Identifikation zu Zwecken der Auskunft bei einem Privatunternehmen gehört nicht dazu. Der Berliner Beauftragte für Datenschutz und Informationsfreiheit bestätigte, dass sich der Springer Verlag an die Behörde gewandt hat. Allerdings konnte diese keinen Missbrauch des Auskunfts- und Widerspruchsrechts durch den einzelnen Anfragenden erkennen. Die Datenschutzanfragen müssten daher bearbeitet und beantwortet werden. Zur Anforderung einer Kopie des Ausweises erläutert die Datenschutzbehörde, dass die angefragte Stelle zwar grundsätzlich „die Identität des Auskunft Begehrenden zu überprüfen“ habe, um nicht Daten an einen Unbefugten gelangen zu lassen. Stimme allerdings die vom Betroffenen angegebene Postadresse mit der gespeicherten Adresse überein, so gebe es regelmäßig keinen Anlass zu weiteren Nachforschungen oder sogar zur Vorlage einer Kopie des Personalausweises. Man werde das Schreiben der Axel-Springer AG zum Anlass nehmen, „den Vorgang aufsichtsrechtlich zu überprüfen“ (Heidrich www.heise.de 13.07.2012).

Berlin

SPD-Nutzerdaten gehackt

Hacker sind in das Computernetz der SPD-Parteizentrale in Berlin eingedrungen und haben Zugangsdaten samt Passwörtern von den Nutzenden erbeutet. Zu dem Angriff kam es im April 2012. Der Server wurde nach Angaben eines Parteisprechers sofort vom Netz genommen. Demnach wurden mindestens 1.900 Zugangsdatensätze gestohlen und in Auszügen auf einer Internetplattform veröffentlicht. Die SPD hat bei der Staatsanwaltschaft Berlin Strafanzeige gestellt, diese ermittelt wegen des „Ausspähens von Daten“. Unter dem Pseudonym Zyklon B hatte der Täter im Kurznachrichtendienst Twitter schon Wochen zuvor in englischer Sprache damit geprahlt, die „Social Democratic Party of Germany“ gehackt zu haben. Für den Twitter-Account wurde der Standort „Deutschland“ angegeben; das geschmacklose Pseudonym lässt auf eine rechte Gesinnung des Hackers schließen. Auf Twitter prahlte er mit weiteren erfolgreichen Einbrüchen u. a. in Websites der NASA, deren europäischem Pendant ESA und der U.S.Airforce. In einer Art Erklärung zu den jüngsten Feldzügen behauptet eine erstmals in Erscheinung getretene Gruppe „The Unknowns“, man wolle mit den Attacken v. a. auf Sicherheistlücken hinweisen (Der Spiegel 21/2012, 16; SZ 21.05.2012, 6; www.heise.de 20.05.2012).

Hamburg

SPD will Polizeirecht verschärfen

Ein Vorschlag der SPD zur Novellierung des Hamburger Polizeirechts enthält einige datenschutzrechtliche Verschärfungen. Umfangreiche Änderungsvorschläge der Fraktion der Grün-Alternativen Liste (GAL) wurden ebenso wie die Hinweise aus der Expertenanhörung im Innenausschuss zurückgewiesen. Besonders einschneidend sind nach Ansicht von Antje Möller, innenpolitische Sprecherin der GAL, die Eingriffe zur sog. „crowd control“ durch Videoüberwachung, Identitätsfeststellungen, Durchsuchungen, Kennzeichen-Scanning und Online-Durchsuchungen. Es werde nicht einmal anstandshalber zwischen „Störern“ und „Nicht-Störern“ unterschieden: „Ansätze für eine Stärkung der Bürgerrechte gegenüber der Polizei fehlen völlig. Anders als in Berlin oder Rheinland-Pfalz fehlt dem Senat in Hamburg der politische Wille, eine individuelle Erkennbarkeit auch in Einsatzzügen im Polizeirecht zu verankern oder eine Öffnung der Polizei für eine wirksame parlamentarische Kontrolle ihres Handelns zu etablieren.“

2005 hatte die damalige CDU-Alleinregierung massive Verschärfungen eingeführt, es sollte das „schärfste Gesetz der Republik“ werden und verfehlte diesen Anspruch nicht (DANA 1/2005, 21f). 2008 vereinbarten GAL und CDU einige Entschärfungen. Kernpunkte waren die Anpassung an die geltende Rechtsprechung des Bundesverfassungsgerichts sowie Fristverkürzungen für Aufenthaltsverbote und Ingewahrsamnahmen, doch konnte keine Einigkeit für einen Entwurf erreicht

werden, weil die CDU die Gelegenheit nutzen wollte, an anderer Stelle neue Verschärfungen einzuführen.

Mit der SPD-Novellierung sollen die Eingriffsschwellen für polizeiliche Maßnahmen gesenkt werden: Durften bei öffentlichen Veranstaltungen und Ansammlungen bisher nur „die für eine Gefahr Verantwortlichen“ per Video von der Polizei überwacht werden, so soll diese Einschränkung künftig wegfallen. Alle Teilnehmenden geraten ins Videovisier der Polizei (§ 8 PolDVG). In „Gefahrengebieten“ wie der Reeperbahn soll die Polizei künftig nicht nur Menschen anhalten und befragen, sondern künftig auch durchsuchen dürfen, wenn die Polizei das für angemessen hält (§ 4 PolDVG). Die Unverletzbarkeit der Wohnung kann schon aufgehoben werden, um eine Identität festzustellen. Die verdeckte Online-Überwachung von Computern soll eingeführt werden. Das massenhafte Scannen von Kfz-Kennzeichen ist vorgesehen (§8a PolDVG). Drei der vier Experten, die im Innenausschuss zu diesen Verschärfungen des Polizeirechts gehört wurden, kritisierten den SPD-Entwurf stark. Die Maßgabe des Bundesverfassungsgerichts, nach der ein Eingriff der Polizei mit der Verletzung der Bürgerrechte abgewogen werden und verhältnismäßig sein muss, wurde als nur teilweise gelungen eingeschätzt. Die Begründungen für polizeiliche Maßnahmen verließen oft den Rahmen der Gefahrenabwehr und verwischten die Grenze zum Strafrecht (www.gal-fraktion.de 23.05.2012).

Hamburg

Bußgeld für Europcar wegen unzulässiger Mietwagen-GPS-Ortung

Der Hamburgische Beauftragte für Datenschutz Prof. Johannes Caspar hat gegen den Autovermieter Europcar ein Bußgeld in Höhe von 54.000 Euro verhängt, weil dieser die wertvollen Pkw aus seiner Flotte ohne Wissen der Mieter per GPS orten ließ. Durch eine Beschwerde war bekannt geworden, dass der Autoverleih in 1.300 hochwertigen Fahrzeugen seiner Flotte Ortungssysteme eingebaut hatte und damit die Mieter und Insassen ohne deren Wissen lokalisierte. Europcar rechtfertigte die Erhebung der Ortungsdaten mit der Möglichkeit der Aufklärung von Diebstählen. Außerdem sollte kontrolliert werden, ob sich der Mieter noch im zulässigen Gebiet befindet. Gerade bei teuren Pkw sind Fahrten in bestimmte Staaten vertraglich untersagt. Außer dem Standort wurden Datum, Zeit und auch die Geschwindigkeit der Fahrzeuge erhoben.

Die Datenschutzbehörde monierte außerdem, dass eine erste Stellungnahme von Europcar unvollständig war. Eine Kontrolle bei einer Firma in Schleswig-Holstein, die im Auftrag von Europcar seit 2004 die Fahrzeugortung vornimmt, ergab, dass die Pkw auch ohne Anlass regelmäßig alle 48 Stunden geortet wurden. Automatisch wurde die Position übermittelt, sobald sich ein Fahrzeug einem Hafengebiet näherte. Caspar kommentierte: „Grundsätzlich ist die Motivation von Europcar nachvollziehbar. Die heimliche Ortung von Mietfahrzeugen und die heimliche Kontrolle der Mieter stellen jedoch einen schweren Eingriff in deren Persönlichkeitsrecht dar. Der Autovermieter hat es dadurch in der Hand, Bewegungsprofile seiner Kunden zu erstellen. Insbesondere durch die anlasslose Ortung werden die Mieter regelmäßig unter einen Generalverdacht gestellt.“ Eine Ordnungswidrigkeit lag darin, dass die GPS-Ortung ohne Wissen und ohne Einwilligung der Mieter erfolgte. Zudem hatte es zwischen Europcar und der ausführenden Firma in Schleswig-Holstein keinen Vertrag zur Auftragsdatenverarbeitung nach dem Bundesdatenschutzgesetz gegeben.

Noch einmal Caspar: „Der Einsatz von Ortungssystemen bei Mietfahrzeugen setzt zumindest eine vollständige Information über Art und Weise der Ortung sowie die ausdrückliche Einwilligung der Betroffenen in das Tracking voraus. Jeder Mieter muss das Recht haben, selbst darüber zu entscheiden, ob er Fahrzeuge anmieten will, deren Nutzung beim Vermieter oder dessen Vertragspartnern unmittelbar eine individuelle digitale Nutzungsspur hinterlässt. Diese Vorgaben werden nun von Europcar erfüllt.“ Inzwischen hat Europcar auch die regelmäßige Ortung alle 48 Stunden abgestellt. Der Übermittlung der Daten in so genannten „Alarmfällen“ muss der Mieter nun vorher ausdrücklich zustimmen. Eine Europcar-Sprecherin erklärte, ihr Unternehmen werde das Bußgeld von 54.000 Euro umgehend zahlen. Die billigste Variante der Mercedes S-Klasse steht derzeit mit 71.876 Euro (netto: 60.400 Euro) im Angebot der Schwaben – mögliche Großkundenrabatte unberücksichtigt (www.heise.de 17.07.2012; PE HmbBfDI 17.07.2012).

Hamburg

Mosley zeigt Google wegen Fotoveröffentlichung an

Der frühere Motorsport-Präsident Max Mosley zeigte Verantwortliche des Suchmaschinen-Giganten Google in Deutschland und in den USA bei der Staatsanwaltschaft Hamburg an, weil sein höchstpersönlicher Lebensbereich verletzt werde. Google macht weiterhin Internet-Nutzenden Fotos zugänglich, die Mosley bei einer privaten Sex-Party zeigen. Das inzwischen eingestellte britische Skandalblatt „News of the World“ hatte Mosley 2008 mit einer Minikamera bei der Party filmen lassen und die Fotos auch im Netz veröffentlicht. Die Bilder wurden in diversen Gerichtsverfahren als illegaler Eingriff in die Intimsphäre eingestuft, sind aber auf verschiedenen Internetseiten noch immer zu finden. Google macht die Fotos über seine Bildersuche zugänglich. Mosleys Anwältin Tanja Irion meint, dass sich der Konzern damit selbst auch strafbar mache. Zuvor hatte Mosley schon ein Zivilklage gegen Google eingereicht und verlangt, dass der Konzern die Fotos über einen Filter aussortiert und nicht mehr anzeigt. Der Konflikt ist ein Präzedenzfall für die Frage, ob und inwieweit Suchmaschinen für die Inhalte Dritter haften. Bereits 2008 hatte die Staatsanwaltschaft Berlin in der Sache ermittelt. Damals hatte Mosley gegen den Axel-Springer-Verlag Strafanzeige eingereicht. Es kam zu einer außergerichtlichen Einigung. Eine Google-Sprecher meinte: „Wir denken, dass diese Anzeige

völlig aussichtslos ist.“ In Italien wurden zwei Jahre zuvor drei Google-Manager zu 6 Monaten auf Bewährung verurteilt, weil auf Googles Video-Portal Youtube ein Film gezeigt wurde, in dem ein behinderter Junge von Mitschülern misshandelt wurde und der nach Ansicht der Kläger nicht rechtzeitig entfernt worden war (Der Spiegel 28/2012, 73; zu News of the World vgl. DANA 2/2011, 86 f.).

Niedersachsen

Checkliste soll extremistische Islamisten erkennbar machen

Mit einer Broschüre „Radikalisierungsprozesse im Bereich des islamistischen Extremismus und Terrorismus“, die der Verfassungsschutz u. a. an Lehrkräfte und JugendamtsmitarbeiterInnen verteilen soll, will das Innenministerium in Niedersachsen den islamistischen Extremismus bekämpfen. An einer Checkliste darin entzündet sich heftige Kritik. Sie listet auf, woran man erkennen soll, dass junge Muslime in den Extremismus abrutschen. Die Kritik entzündete sich vor allem an dort aufgeführten Punkten wie „Gewichtsverlust durch veränderte Essgewohnheiten“ oder „längere Reisen in Länder mit mehrheitlich muslimischer Bevölkerung“. Auch eine „intensive Beschäftigung mit dem Leben nach dem Tod“, plötzlicher Reichtum oder plötzliche Schulden können demnach auf eine Radikalisierung hinweisen. Hat ein Muslim plötzlich einen anderen Kleidungsstil? Ist er sportlicher geworden? Lernt er arabisch? Muslime, die ohnehin schon fünfmal täglich beten, machen sich laut Broschüre durch „zunehmend strengere Religionsauslegung“ suspekt. Verdächtig sind auch die, die sich bemühen, „besondere Umstände der Lebensführung oder Freizeitgestaltung zu verheimlichen“, also die Wert auf ihre Privatsphäre legen. Die Broschüre richtet sich an die Partner in der Islamismusprävention, die in ihrer täglichen Arbeit oder in ihrem sozialen Umfeld Radikalisierungsprozesse erkennen könnten. Dazu gehörten Lehrkräfte, Mitarbeitende von Jugend- und Ausländerbehörden sowie von muslimischen Einrichtungen und Organisationen. Die Adressaten werden aufgefordert, „in gebotenen Einzelfällen konkrete fallbezogene Informationen über die betroffene Person zwischen den Kooperationspartnern und den Sicherheitsbehörden auszutauschen“.

Muslime, Gewerkschafter und die Opposition im Landtag kritisierten die Checkliste mit den etwa 30 „Radikalisierungsmerkmalen“. Der Berliner Ver.di-Gewerkschaftssekretär Christian Goetz stellte fest: „Das verstößt gegen die Persönlichkeitsrechte jedes Einzelnen! Jeder Bürger hat den Anspruch und das Recht auf Privatsphäre und die Entfaltung der Persönlichkeit. Wenn dann da Menschen sind, die diese Dinge als Aufforderung verstehen, werden Anzeigen vermehrt vorkommen.“ Mit der Broschüre unterwandere das Innenministerium Grundrechte. Der Osnabrücker Islamwissenschaftler Bülent Ucar meinte, mit solchen allgemein etwa an Schulen verteilten Listen werde das Thema Islamismus dramatisiert: „Das führt dazu, dass viele religiös lebende Muslime zu unrecht verdächtigt werden“. Die Kriterien seien abwegig. Prävention vor Extremismus sei natürlich eine staatliche Aufgabe. „Das ist aber ein sensibles Feld, das man angesichts der herrschenden islamkritischen Atmosphäre mit Fingerspitzengefühl bearbeiten muss. Ich rate zu mehr Gelassenheit und Behutsamkeit.“ Er halte es für besser, auf konkrete Hinweise von LehrerInnen oder JugendarbeiterInnen zu reagieren. Der Vorsitzende des niedersächsischen Moscheenverbands Schura, Avni Altiner sagte: „Die Liste fördert ein Klima der Angst“. In der Broschüre heißt es vieldeutig, die Liste der Radikalisierungsmerkmale könne „jedoch nicht als abschließend oder als in ihrer Aussagekraft absolut angesehen werden“ – denn offenbar wird die Suche nach Terroristen dadurch erschwert, dass gewaltbereite Islamisten versuchten, ein „nach außen recht unauffälliges Leben zu führen“. Emine Oguz vom türkisch-muslimischen Verband Ditib meinte, die Broschüre schüre Islamfeindlichkeit.

Rainer Hämmer, stellvertretender Landesdatenschutzbeauftragter von Niedersachsen, sieht in dieser Broschüre nicht in erster Linie ein datenschutzrechtliches Problem. „Die Aufforderung an die Mitbürger, bestimmte Personengruppen zu beobachten und gegebenenfalls zu melden, wird zunehmend zu einem gesellschaftspolitischen Problem“. In datenschutzrechtlicher Verantwortung stehe jeder, der etwas meldet, wobei vor allem Arbeitgeber sich zuvor im Bundesdatenschutzgesetz informieren müssten. „Für Bedienstete der niedersächsischen Behörden, also Lehrer, sehe ich rechtlich keine Befugnis, Informationen über ihre Schüler weiterzuleiten.“ Bei Privatpersonen seien Meldungen dann zulässig, wenn Gefahr für Leib und Leben bestehe. „Da es sich nach der Liste lediglich um Indizien von einem Laien handelt, ist die Weitergabe von Informationen hier nicht zulässig.“

Die stellvertretende innenpolitische Sprecherin der SPD-Landtagsfraktion, Sigrid Leuschner, sprach von einer „absurden Idee“: „Dieser Ansatz trägt unverkennbar die Handschrift von Innenminister Schünemann, der praktisch seit seinem Amtsantritt vor neuneinhalb Jahren Vorbehalte, Vorurteile und Misstrauen gegenüber muslimischen Mitbürgern fördert und schürt.“ Die migrationspolitische Sprecherin der Grünen, Filiz Polat, sagte, der Minister versuche, die Muslime unter den Generalverdacht des Extremismus zu stellen. Sie forderte Schünemann auf, die Broschüre „einzustampfen“. Die Fraktion Die Linke forderte, der Minister solle gemeinsam mit den muslimischen Verbänden und Gemeinden Konzepte gegen radikalen Islamismus erarbeiten.

Das Innenministerium wies die Kritik zurück. Justiz und Schulen hätten solche „Handreichungen“ angefragt. Es sei nicht zielführend, einzelne Formulierungen aus der Broschüre als Basis für eine grundsätzliche Kritik heranzuziehen. Auch muslimische und nichtmuslimische Organisationen und Einrichtungen hätten immer wieder gefordert, den Gefahren von Radikalisierungen möglichst frühzeitig zu begegnen (www.welt.de 28.06.2012; Sayhi www.taz.de 28.06.2012).

Niedersachsen

Facebook-Zwang an Schule in Braunlage

In einer kleinen Randnotiz in der Goslarschen Zeitung wurde berichtet, dass in Braunlage im Harz sechs

SchülerInnen der Wurmbergschule von einer Unterrichtsstunde mit einem Geschichtenerzähler ausgeschlossen worden sind, weil ihre Eltern einer Veröffentlichung von Fotos der Veranstaltung bei Facebook nicht zugestimmt hatten. Eltern, Medien und Schulen tun sich scheinbar weiterhin mit dem Thema schwer, inwieweit Kinderbilder auf sozialen Plattformen wie Facebook veröffentlicht werden dürfen. Eltern posten teilweise sorglos die Bilder ihrer Kinder bei Facebook, andere wie die Facebook-Gruppe „Keine Kinderfotos im Social Web“ sehen sich in der Pflicht, ihre Kinder vor der Veröffentlichung ihrer Bilder zu schützen – sei es auf eigenen Seiten der Eltern, auf fremden Seiten wie der des Geschichtenerzählers oder auf der Facebook-Seite der Schule oder des Kindergartens. Dass mit der Veröffentlichung gewisse Rechte am Bild an Facebook übertragen werden, ist dabei nur ein Nebenaspekt. Für den Initiator der Gruppe geht es vor allem um die Privatsphäre des Kindes, die die Eltern schützen sollen: „Vermutlich herrscht Konsens, dass es sich nicht gehört, über andere im Web zu plaudern. Warum sollte das also bei (meinen) Kindern anders sein? Weil die mir gehören? Blödsinn! Weil die das selber lustig finden? Blödsinn! Weil die sich nicht wehren und beschweren können? Vermutlich ist da die Lücke.“

Abbildungen von Kindern auf sozialen Plattformen bergen für die Kinder ganz reale Gefahren: Pädophile suchen gezielt bei Facebook nach Opfern. Das Familienhandbuch des Staatsinstituts für Frühpädagogik (IFP) zitierte aus einer Studie zur potenziellen Nutzung der Fotos durch Pädophile. „86,1 Prozent der Teilnehmer (gaben) an, Bildmaterial aus dem legalen und/oder illegalen Bereich zu nutzen.“ Eltern müssen grundsätzlich gefragt werden, bevor Bilder ihrer Kinder auf Facebook gepostet werden. Das gilt auch für die Seiten der Schulen. Facebook-Seiten von Schulen halten DatenschützerInnen allerdings generell für rechtlich unzulässig und sind empört, dass es sie trotzdem gibt. In einer Erklärung vom 17.04.2012 bezeichnete der schleswig-holsteinische Landesdatenschützer Thilo Weichert Facebook-Seiten von Schulen als „pädagogisch katastrophales Vorbild für die Kinder und Jugendlichen. Facebook legt alles darauf an, nicht nur den Kindern, sondern auch den Schulleitungen den Kopf zu verdrehen.“

Vor der grundsätzlich schriftlichen Einwilligung zur Veröffentlichung von Kinderbildern durch die volljährigen SchülerInnenn und bei Minderjährigen durch deren Eltern müssen die Betroffenen über die Risiken wie weltweite Abrufbarkeit, Veränderbarkeit und Nutzung in anderen Zusammenhängen ausreichend informiert werden. Es ist zu vermeiden, dass weitere Informationen über das Kind, insbesondere Wohnadressen, private E-Mail-Adressen und Ähnliches mitveröffentlicht werden.

Dass Kinder von schulischen Aktivitäten ausgeschlossen werden, weil ihre Eltern der Veröffentlichung ihrer Bilder nicht zugestimmt haben – so wie es in Braunlage im Harz geschehen ist –, ist für Weichert nicht akzeptabel. „Ich bin entsetzt. Als Datenschützer allgemein und bürgerrechtlich bewusster Mensch kann ich das Verhalten nicht nur aus rechtlicher, sondern vor allem aus pädagogischer Sicht nur kritisieren: Die zwangsweise Animation von Kindern, ein Medium zu nutzen, das für diese weder rechtlich vorgesehen und erlaubt noch geeignet ist, müsste meines Erachtens nicht nur öffentlich kritisiert, sondern aufsichtlich gerügt werden.“ Nach Ansicht eines Sprechers der Fröbel-Gruppe erklärt, die Krippen, Kindergärten und Horte mit rund 11.000 Kindern in mehreren Bundesländern betreibt, gibt es genügend Möglichkeiten sicherzustellen, dass die Bilder der Kinder nicht auf Facebook erscheinen: „Wir würden bei der Dokumentation sicherstellen, dass manche Kinder nicht mit aufs Bild kommen, oder in einer nachträglichen Abstimmung Bilder aussortieren, auf denen Kinder zu sehen sind, bei denen das Eltern nicht wünschen. Hier geben die Eltern als Erziehungsverantwortliche vor, was für die Kinder gewünscht ist oder nicht“ (Sawall, Gunardono www.zeit.de 20.06.2012; www.golem.de 20.06.2012; www.goslarsche.de 18.06.2012).

Nordrhein-Westfalen

Vorwurf gegen Frauenarzt: Patientinnen intim gefilmt

Die Staatsanwaltschaft in Dortmund ermittelt gegen einen Frauenarzt, der mit Mini-Kameras in einer Armbanduhr und einem Kugelschreiber heimlich intime Fotos und Videos von Patientinnen aufgenommen haben soll. 9 Frauen haben bislang Anzeige erstattet. Die Ermittler gehen davon aus, dass es noch weitere Geschädigte gibt. Zwecks Erlangung weiterer Erkenntnisse werden der Praxis-Computer sowie CDs und DVDs des 41-jährigen Gynäkologen ausgewertet wegen des „Verdachtes der Verletzung des höchstpersönlichen Lebensbereichs durch Bildaufnahmen“ (SZ 25.07.2012, 9).

Sachsen

Thierses Polizeibewertung in Polizeidatei nicht gelöscht

Bundestags-Vizepräsident Wolfgang Thierse (SPD) erfuhr durch Zufall, wie eigenmächtig die sächsische Polizei mit personenbezogenen Daten umgeht. Er wollte nach dem Dresdner „Handygate“ im Februar 2011 eigentlich nur wissen, ob von ihm Mobilfunkdaten gespeichert worden sind (vgl. DANA 3/2011, 119 ff.). Das sei nicht der Fall, teilte man ihm mit. Wohl aber finde sich eine Speicherung im Polizeilichen Auskunftssystem Sachsen (PASS): „Ereignis: StGB § 187 Verleumdung – ohne sexuelle Grundlage“, dazu die Feststellung: „Der Vizepräsident des Deutschen Bundestages hat die sächsische Polizei (…) verleumdet.“ In einem Fernseh-Interview hatte Thierse zuvor beklagt, dass die Demonstrationsrechte von GegnerInnen des Nazi-Aufmarsches eingeschränkt gewesen seien. Die Polizei sei vollauf beschäftigt gewesen, die Neonazis zu schützen: „Das ist sächsische Demokratie.“

Ein ranghoher Polizeibeamter meinte, Thierse habe damit Sachsens

PolizistInnen beleidigt, und stellte gegen ihn Strafanzeige. Auch die beiden großen Polizeigewerkschaften äußerten harsche Kritik. Der Vorsitzende der Deutschen Polzeigewerkschaft (DPolG), Rainer Wendt, forderte Thierses Rücktritt. Er sei eine „Schande für das deutsche Parlament“. Die Staatsanwaltschaft Dresden ermittelte – und stellte das Verfahren gleich wieder ein. Ein strafbares Verhalten liege nicht vor, weil die Äußerung von der Meinungsfreiheit gedeckt sei. Dass die Polizei die Demonstration von Nazis schütze, sei eine Tatsache. Die Äußerung über die „sächsische Demokratie“ sei von der Meinungsfreiheit nach Art. 5 des Grundgesetzes gedeckt.

Thierse war erstaunt, dass er mit dieser Geschichte immer noch im Polizeicomputer auftauchte, da die Daten längst hätten gelöscht sein müssen. Er schrieb dem Landeskriminalamt (LKA), er sei „außerordentlich befremdet“. Das LKA leitete den Wunsch an die Polizeidirektion Dresden weiter. Die teilte Thierse Ende Juni 2012 mit, die gespeicherten Daten seien nun „vollständig gelöscht“ worden - fast anderthalb Jahre, nachdem die Staatsanwaltschaft nicht mehr wegen Thierses Äußerung über „die sächsische Demokratie“ ermittelte. Die Ermittlungsakte sei „physisch vernichtet“ worden. Die Polizeidirektion Dresden wollte auf eine Presse-Anfrage nicht Auskunft geben, ob es üblich ist, dass zu löschende Daten nicht gelöscht werden (Erb www.taz.de 02.07.2012).

Schleswig-Holstein

Milde Sanktion für unerlaubt schnüffelnden Polizisten

Um Belastungsmaterial für einen privaten Rechtsstreit gegen einen lästigen Mieter zu beschaffen, hat ein 57jähriger Kripobeamter aus Neumünster in Schleswig-Holstein gegen das Bundesdatenschutzgesetz (BDSG) verstoßen und muss hierfür eine Geldbuße von 1000 Euro bezahlen. Der Polizeibeamte erlangte im November 2011 vom Netzbetreiber „Kabel Deutschland“ widerrechtlich Informationen über Zahlungsversäumnisse eines ungeliebten Mieters, indem er dienstliche Interessen vorspiegelte. Die Informationen ließ er sich direkt an seine dienstliche Faxnummer in der Polizeibehörde und per E-Mail auf den Dienst-PC senden. Der Anwalt des Mieters wurde stutzig, als der Beamte die rechtswidrig erlangten Auskünfte im Zivilstreit um die Einrichtung eines Fernsehanschlusses für den Mieter einsetzte. Der Ausspionierte erstattete Strafanzeige, doch die Anklagebehörde wollte den Verstoß gegen das BDSG zunächst nicht ahnden. Erst die Beschwerde bei der Generalstaatsanwaltschaft führte zur Beantragung eines Strafbefehls. Der Kripomann legte hiergegen Beschwerde ein und fand einen milden Richter, der das Verfahren gegen Zahlung einer Geldbuße von 1000 Euro einstellte.

Im Vorfeld des Verfahrens hatte der Polizeibeamte dem Beamten schriftlich angedroht, er betreibe seine Nachforschungen „so lange weiter, bis Sie endlich ausgezogen sind“. Während bei der Kieler Staatsanwaltschaft „keine weiteren ähnlich gelagerten Fälle bekannt“ waren, meinte der Rechtsanwalt des Mieters, dass Verstöße gegen den Datenschutz in Verwaltungsbehörden an der Tagesordnung seien. So sollen sich Duisburger Polizeibeamte im Nebenjob als Versicherungsmakler Privatadressen potenzieller KundInnen verschafft haben. Andere sollen für ihre Tätigkeit als Security-Mitarbeiter „dienstlich“ ermittelt haben. Ein Beamter setzte seine minderjährige Tochter über das umfangreiche Vorstrafenregister ihres neuen Verehrers in Kenntnis (Geyer, Kieler Nachrichten 08.08.2012, 1, 11).

Datenschutznachrichten aus dem Ausland

Weltweit

Facebook durchsucht Chat-Protokolle

Um kriminelle Aktivitäten in der gigantischen Datenmenge der 900 Mio. Mitglieder aufzuspüren, durchsucht Facebook automatisiert die Kommunikation seiner Mitglieder. Facebooks oberster Sicherheitschef Joe Sullivan teilte mit, Facebook setze eine Technologie ein, die automatisiert private Kommunikation überwacht und nach bestimmten Schlüsselbegriffen durchsucht. Facebook greife dazu auf ein Archiv an Chatprotokollen zurück, die sexuellen Übergriffen vorausgegangen seien. Sollte sich eine ähnliches Gespräch erneut entwickeln, so würden Facebook-Mitarbeiter automatisch benachrichtigt. Sie entschieden dann, ob der Fall an die zuständigen Strafermittlungsbehörden weitergegeben werde. So sei es beispielsweise möglich gewesen, im vergangenen März einen Floridaner zu überführen, der mit einer 13-Jährigen über Sex geschrieben und sich mit ihr für den darauffolgenden Tag verabredet habe. Wie intensiv eine Unterhaltung durchleuchtet werde, hänge davon ab, wie Facebook die Beziehung zwischen den beteiligten Nutzern einschätzt. Die Mitteilungen Sullivans legen nahe, dass vor allem Unterhaltungen zwischen Personen, von denen Facebook ausgeht, dass sie nicht auf realen Bekanntschaften basieren, betroffen sind. Neben verdächtigen Formulierungen werden Aspekte in der Beziehung der beteiligten Kommunikationspartner, z. B. das unterschiedliche Alter, herangezogen. Über diese Überwachung ihrer Kommunikation unterrichtet Facebook seine Mitglieder nicht.

Letztendlich sei man nur in der Lage, einen Bruchteil der kriminellen Absichten bereits im Voraus aufzu-

spüren. Vor allem wolle Facebook vermeiden, Nutzende zu beschuldigen, die sich hinterher als unschuldig herausstellten. Das bedeute, dass die Kriterien, nach denen eine Unterhaltung als gefährlich eingestuft wird, nicht zu streng sein dürften. Facebook teilte zunächst auf Anfrage mit, dass das Unternehmen auch in Deutschland „proaktiv“ auf die Ermittlungsbehörden zugehe, falls es von einer vermeintlichen oder tatsächlichen Straftat erfahre. Später wurde bekannt gegeben, nochmals überprüfen zu wollen, ob tatsächlich proaktiv auf deutsche Behörden zugegangen werden soll, wenn es eine mögliche Straftat erkannt zu haben glaubt.

Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit in Rheinland-Pfalz Edgar Wagner ist nicht begeistert: „So unterstützenswert das Ziel ist, sexuelle Belästigungen oder Schlimmeres zu verhindern, so muss dies doch rechtskonform erfolgen. Eine Stelle, deren Aufgabe das Ermöglichen von Kommunikation ist, darf sich solche Überwachungen nicht anmaßen. Man stelle sich vor, die Telekom würde alle Telefonate unter ähnlichen Aspekten prophylaktisch überwachen. Ein solches Vorgehen ist mit unserer Rechtsordnung unvereinbar.“ Facebook unterliege in Deutschland dem Telekommunikationsgeheimnis, das dem Diensteerbringer untersage, sich Kenntnis vom Inhalt der Telekommunikation zu verschaffen, soweit dies nicht der Diensteerbringung selbst dient. Völlig unklar sei, ob und wie lange solche ja lediglich vagen Verdachtsfälle gespeichert blieben und an wen die Daten weitergegeben würden. Facebook dürfe sich nicht die Befugnisse anmaßen, die allein den Strafverfolgungsbehörden zustehen und sich selbst zum Hilfssheriff ernennen. Zudem müsse auf jeden Fall vermieden werden, dass Nutzer ungerechtfertigt verdächtigt werden. Fälle wie der des Sozialarbeiters, der fälschlicherweise in Verdacht geriet, weil er auffällig viele minderjährige Facebook-Freunde - die von ihm betreuten Jugendlichen - hatte, belegten, welche Gefahren hier bestehen (Menn http://www.reuters.com 12.07.2012; Paukner www.süddeutsche.de 13.07.2012; LfDI Rheinland-Pfalz PE v. 19.07.2012).

Großbritannien

Polizei durchsucht Handys mit Cellphone-Dumpern

Britische Behörden haben begonnen, in großem Stil sogenannte Cellphone-Dumper zu kaufen, um die auf Mobiltelefonen gespeicherten Daten auslesen zu können. Die Londoner Polizei kann damit künftig innerhalb von circa 20 Minuten Mobiltelefone von Verdächtigen durchsuchen und darauf vorhandene Daten wie Anruflisten, Bilder, Videos, SMS, E-Mails sowie Informationen aus sozialen Netzwerken extrahieren. Auch bereits gelöschte Informationen lassen sich damit wiederherstellen. Möglich ist das dank eines Systems namens Aceso Kiosk des Herstellers Radio Tactics. Der britische Anbieter der Forensik-Geräte warb im April 2012 damit, dass in allen 16 Stadtteilen Londons Polizeistationen entsprechend ausgestattet werden. 300 BeamtInnen der Metropolitan Police würden im Umgang mit der Technik geschult. Zuvor hatte schon die britische Militärpolizei einen Vertrag mit Radio Tactics unterzeichnet zu einer mobilen Variante der Durchsuchungsgeräte namens Aceso Field, mit der deren Soldaten ausgerüstet werden.

BürgerrechtlerInnen sind besorgt, weil so auch die privaten Daten in den Geräten durchsucht und kopiert werden können. Dies ist auch in Großbritannien nicht einfach so erlaubt. Handys dürfen in Deutschland in einem Ermittlungsverfahren beschlagnahmt und untersucht werden, aber nicht allein auf der Basis eines vagen polizeilichen Verdachts. Die britische Polizei scheint mit dem Thema eher pragmatisch umzugehen. In einer Pressemitteilung wird Stephen Kavanagh, Deputy Assistant Commissioner der Metropolitan Police, wie folgt zitiert: „Mobiltelefone und andere Geräte werden zunehmend bei allen möglichen kriminellen Aktivitäten genutzt. Wenn ein Verdächtiger festgenommen wird, und wir bei ihm ein Mobiltelefon finden, von dem wir glauben, dass es bei einem Verbrechen benutzt wurde, haben wir es bisher in eines unserer Forensiklabors geschickt.“ Dank des neuen Systems jedoch hätten Beamte „sofortigen Zugang“ zu den Informationen und könnten sie für Ermittlungen nutzen. Jedes Mobiltelefon könnte in Zukunft auf diese Art untersucht werden, was nicht nur für politische Aktive eine Horrorvorstellung sein dürfte, die auf einer Demo vorübergehend festgehalten werden. Die BBC berichtete, dass die Metropolitan Police die abgesaugten Daten womöglich anschließend speichert, selbst wenn der Verdächtige wieder freigelassen wird.

Wie die Technik eingesetzt werden kann, demonstrierten Beamte der State Police im US-amerikanischen Bundesstaat Michigan, die schon bei geringen Verkehrsverstößen die Handys der Betroffenen abforderten und deren Daten kopierten. Die entsprechenden Geräte sind, so die Bürgerrechtsgruppe American Civil Liberties Union (ACLU), bereits seit 2008 bei der State Police im Einsatz. Das System namens CelleBrite UFED ähnelt in der Funktion dem britischen Modell und kann genauso viele Daten auslesen. Auch das amerikanische Heimatschutzministerium spioniert seit Jahren routinemäßig Laptops und Mobiltelefone von Einreisenden an Flughäfen aus, ohne Verdacht und ohne Durchsuchungsbeschluss.

Die Systeme nutzen bekannte Schwachstellen und die in die Software mancher Telefone eingebauten Wartungsschnittstellen, um an den Flashspeicher zu gelangen. In manchen Fällen wird auch zuerst eine Software auf das Gerät gespielt, die anschließend die Daten herausreicht. Für jeden Telefontyp muss daher ein eigener Zugangsweg entwickelt und im Zweifel aktualisiert werden, wenn der Hersteller die Lücke schließt. Hat der Scanner jedoch erst einmal Zugang zum Speicher des Telefons, liest er alle Daten aus und erstellt eine vollständige Kopie der Festplatte. Zwar kann vor Scannern wie Aceso und CelleBrite ein Passwort schützen. Doch längst nicht alle Nutzenden sichern ihre Geräte damit. Passwörter sollten hinreichend lang und komplex sein, damit sie nicht geknackt werden können. Sicherer ist es, die Speicher im Gerät zu verschlüsseln, was bei neueren Versionen des Betriebssystems Android möglich ist (Biermann www.zeit.de 05.06.2012).

Tschechien

Aus für elektronische Gesundheitskarte

In Tschechien ist das Projekt einer elektronischen Gesundheitskarte nach 10 Jahren wegen Korruptionsvorwürfen, Datenschutzbedenken und der mangelnden Akzeptanz bei den PatientInnen gescheitert. Vor 10 Jahren plante die damalige sozialdemokratische Regierung in Prag, Diagnosen, Laborbefunde und Röntgenbilder auf dem Chip der Karte zu speichern, so dass ÄrztInnen und die Krankenkassen diese Daten jederzeit abrufen können. Der stellvertretende Gesundheitsminister Petr Nosek teilte nun mit: „Wir haben uns entschieden, das Projekt der elektronischen Krankenkarte zu beenden. Die Speicherung der Patientendaten in großen Datenzentren ist nicht mehr zeitgemäß. Außerdem ist die Finanzierung sehr undurchsichtig.“ Mehr als 80 Millionen Euro sind seit Projektbeginn investiert worden. Das Interesse der PatientInnen war von Anfang an äußerst verhalten. Nur die staatlich kontrollierte Krankenkasse VZP war zur Teilnahme bereit und überließ es ihren Versicherten, ob sie sich freiwillig an dem Modellprojekt beteiligen. 2,5 Millionen PatientInnen ließen mit den Jahren ihre Daten auf der Karte speichern.

Immer wieder gab es handfeste Korruptionsvorwürfe. Viel Geld ist in dunkle Kanäle geflossen, meinte die kommunistische Abgeordnete Sona Markova: „Das Projekt wurde damals nicht öffentlich ausgeschrieben und ist deshalb absolut überteuert. Es gab bei der Finanzierung viele undurchsichtige Manipulationen. Die Karte hat ihren Zweck nicht erfüllt.“ In den tschechischen Medien wurde zudem immer wieder über den laxen Umgang mit den Patientendaten berichtet. Obwohl dieses Datenschutzproblem auch in den zuständigen Ministerien bekannt war, schafften es alle Nachfolgeregierungen nicht, die Krankheiten des Projektes zu heilen. Die Krankenkasse VZP versuchte schon seit längerem, das Projekt zu beenden, so Vorstandsmitglied Boris Schtastny: „Das Projekt lief leider zehn Jahre - aber niemand wollte sich damit ernsthaft beschäftigen. Es wurde von jedem Minister an seinen Nachfolger weiter gereicht wie eine heiße Kartoffel. Ich bin sehr froh, dass dieses Projekt nun endgültig gestoppt wird.“ Trotz der sofortigen Kündigung kommen auf die Steuerzahlenden in den kommenden Jahren wegen der langen Laufzeiten des Vertrages weitere Kosten zu: Insgesamt müssen noch rund 3,5 Millionen Euro für das gescheiterte Experiment bezahlt werden (Heinlein www.tagesschau.de 30.05.2012).

USA

Millionen Mobilkommunikationsdaten für Ermittlungsbehörden

Im Jahr 2011 haben US-Mobilfunkbetreiber in insgesamt rund 1,3 Millionen Fällen Daten, SMS-Nachrichten und Aufenthaltsorte von Mobilgeräte-Besitzenden an Ermittlungsbehörden weitergegeben. Diese Zahl geht aus einer Antwort von Unternehmen wie AT&T, Sprint oder T-Online USA auf eine Anfrage des Kongresses in Washington hervor. Die Datenherausgabe hat damit gegenüber den Vorjahren deutlich zugenommen. Nicht aufgeschlüsselt wurde, welche Behörden nach den Informationen gefragt haben. Viele Aufforderungen zur Übermittlung von Namen, Nummern und anderer Privatdaten müssten, so der Bericht, ohne gerichtliche Verfügung befolgt werden, da die Behörden sie als Notfall deklarieren. Es seien auch Anfragen darunter, die von den Telekomanbietern als „unangemessen“ zurückgewiesen wurden. Problematisch sei vor allem, dass viele Handys heute mit GPS-Empfängern ausgestattet seien, die den genauen Aufenthaltsort ihrer Nutzenden ermitteln. Nach diesen Daten würden die Behörden oft fragen (www.welt.de 09.07.2012).

USA

Google: nach illegaler Cookiespeicherung Millionenstrafe

Google akzeptierte ein Vergleichsangebot der US-Handelsbehörde Federal Trade Commission (FTC) und verhinderte daduch ein Klageverfahren, weil der Konzern die Datenschutzeinstellungen von Usern umging. Das Unternehmen zahlt 22,5 Millionen Dollar (18,3 Millionen Euro). Hintergrund ist, dass der Suchmaschinenbetreiber eine Lücke im Browser „Safari“ des Konkurrenten Apple ausgenutzt hat, um Nutzenden bestimmte Werbeformate zu präsentieren. Mit einem Trick speicherte Google über seinen Dienst Google+ ein Tracking-Cookie auf den Geräten von Internetnutzenden, selbst wenn diese Cookies bewusst ausgeschaltet hatten. Google verpflichtete sich zudem, alle regelwidrig installierten Cookies zu deaktivieren.

Nachdem im Februar 2012 eine Untersuchung durch den Informatiker Jonathan Mayer die Praxis detailliert beschrieb, hatte Google die Technik abgeschaltet. Dennoch hatte die FTC den Fall ebenso wie die Staatsanwälte mehrerer Bundesstaaten aufgegriffen. Es handelt sich bei dem angenommenen Vergleich um die höchste jemals von der Behörde verhängte Sanktion. FTC-Chef Jon Leibowitz: „Egal wie groß oder wie klein – alle Unternehmen müssen die Anweisungen der FTC befolgen und ihre Datenschutz-Versprechen gegenüber den Verbrauchern halten.“ Bei einem Quartalsgewinn von zuletzt 2,8 Milliarden US-Dollar benötigte Google allerdings nicht einmal einen Tag, um die Millionenbuße zu verdienen. Schwerer wiegt da hoffentlich der Imageschaden (www,spiegel.de 10.07.2012; SZ 11./12.2012, 26; www.heise.de 09.08.2012).

USA

Arbeitgeber fordern Passwörter von sozialen Netzwerken

In den USA werden verstärkt Fälle bekannt, in denen KandidatInnen in Bewerbungsgesprächen aufgefordert werden, Passwörter anzugeben oder sich gar vor Ort einzuloggen, um einen uneingeschränkten Einblick in deren Profile auf sozialen Netzwerken wie Facebook, Google+, Myspace oder LinkedIn zu geben. Selbst der Zugang zu E-Mail-Konten wurde teilweise ge-

fordert. Auch gibt es Beispiele, dass Arbeitgeber versuchten, inkognito als Freunde an Bewerbende heranzukommen, um deren Profil auslesen zu können. Sportstudierende wurden aufgefordert, ihren Trainer oder einen Compliance Officer als „Freund“ zu akzeptieren. Damit soll auch verhindert werden, dass die Studierenden keine unanständigen Dinge bei sozialen Netzwerken veröffentlichen. Insbesondere bei der Suche nach Gefängnispersonal oder Sheriffs war das Anfordern von Zugangsdaten an manchen Orten jahrelang gängige Praxis, aber auch bei der Einstellung von Polizisten in Spotsylvania in Virginia. Als Begründung wurde angegeben, man wolle verhindern, dass in den Gefängnissen kriminelle Bandenmitglieder eingestellt werden. Facebook sprach von einer „Besorgnis erregenden Zunahme von Berichten, dass Arbeitgeber oder andere Interessierte Zugang zu Kundenprofilen erlangen wollen, der ihnen nicht zusteht.“ Es wurde darauf hingewiesen, dass die Pflicht zur Herausgabe von Zugangsdaten gegen die Nutzungsbedingungen von Facebook verstoße. Eric Egan, Datenschutzbeauftragter von Facebook, schrieb in einem Blog, jeder Nutzende müsse wissen, dass er das Recht habe, sein Passwort für sich zu behalten. Er kündigte „juristische Mittel“ an, sollten die Arbeitgeber sich nicht bändigen. Bewerbungsverfahren sind in den USA ein Minenfeld. Diskriminierungsklagen können Millionensummen kosten. Kein Personalbüro darf den Eindruck erwekken, einen Kandidaten wegen persönlicher Merkmale wie Religion, Alter oder Wohnort abgelehnt zu haben. Fotos sind auch tabu. So ist es nicht erstaunlich, dass Arbeitgeber andere Wege suchen, um an aussagekräftige Angaben zu gelangen.

Vor allem junge Menschen stellen in sozialen Netzwerken Daten ein, die sie sonst nur FreundInnen oder ihrem Tagebuch anvertrauen würden und hoffen auf die Datenschutzeinstellungen, die die Öffentlichkeit von entsprechend gekennzeichneten Daten fernhalten sollen. Unternehmen, die nach den Zugangscodes fragen, nutzen die Verzweiflung vieler Bewerbenden aus, die auch dreieinhalb Jahre nach dem großen Wirtschaftscrash in den USA dringend Arbeit suchen. Jobsuchende müssen befürchten, aussortiert zu werden, wenn sie Daten nicht herausrücken. Der an der George Washington University lehrende Professor Orin Kerr verglich die Passwortabfrage damit, als würden Personalchefs die Bewerbenden auffordern, ihren Hausschlüssel zu übergeben. In Maryland wurde die Übung bei der Einstellung von Gefängnispersonal im Jahr 2011 durch eine Klage der American Civil Liberties Union (ACLU) beendet. Die Klage hatte aber zunächst nur zur Folge, dass an Stelle der Herausgabe von Nutzername und Passwort die Bewerbenden gezwungen wurden, sich beim Surfen über die Schulter schauen zu lassen. Die rechtliche Argumentation der Gegner derartiger Praktiken basiert nicht nur auf Privatheits- und Datenschutzerwägungen, sondern auch auf der damit verbundenen Beeinträchtigung der Meinungsfreiheit. Nach Veröffentlichung solcher Praktiken haben die Bundesstaaten Illinois und Maryland Gesetzesvorhaben eingereicht, die zumindest öffentlichen Arbeitgebern verbieten sollen, von Bewerbenden den Zugang zu Netzwerken einzufordern (Der Spiegel 13/2012, 72; Koch SZ 26.03.2012, 1; O´Dell venturebeat.com 21.03.2012; Sullivan redtape.msnbc.msn.com 06.03.2012).

USA

Entwicklung von Mesh-Netzwerken gegen Zensur und Kontrolle in Diktaturen

Die US-Regierung finanziert ein Online-Projekt, mit dem BürgerInnen in repressiven Staaten eigene Netzwerke aufbauen und sich der Überwachung der einheimischen Sicherheitsbehörden entziehen können. Bei den dabei geförderten Mesh-Datennetzen erfolgt die Kommunikation nicht über eine zentralisierte Infrastruktur, bei der über den Mobilfunkbetreiber oder Internet-Anbieter eine Kontrolle der zentralen Leitungen und Austauschpunkte möglich ist. Vielmehr ist jeder der Teilnehmenden ein eigener Knoten. Daten werden so von Gerät zu Gerät weitergegeben, bis die EmpfängerIn erreicht ist – und falls einer der Zwischenknoten ausfallen sollte, wird eben der Weg über die Hardware einer anderen BenutzerIn gewählt. Mesh-Netzwerke sind sehr robust, wenn es eine ausreichende Anzahl von Knoten gibt. Außerdem sind sie effizient, weil sich die Infrastruktur quasi wie von selbst aufbaut. Das Projekt „Commotion Wireless“ („Drahtloser Tumult“), das der Washingtoner Think Tank New America Foundation mit Mitteln der US-Regierung angeschoben hat, will Mesh-Datennetze für den Aufbau alternativer Infrastrukturen in Zensurstaaten und repressiven Regimen nutzen.

Statt auf ein von Geheimdiensten und Polizeibehörden kontrolliertes Internet angewiesen zu sein, sollen sich AktivistInnen mit „Commotion Wireless“ selbst ein eigenes Netzwerk herstellen, über dass sie dann ungestört kommunizieren können. Ein Anschluss an das restliche weltweite Datennetz ist dabei möglich, muss aber nicht sein. Die verwendete Hardware ist sehr einfach: Neben einem kostengünstigen WLAN-Router, auf dem eine von der New America Foundation entwickelte Software läuft, können auch Laptops, Desktop-Rechner mit WLAN-Karte oder Smartphones und Tablets verwendet werden. Selbst einfache GSM-Mobilfunkgeräte lassen sich mit etwas Aufwand und einem – allerdings vergleichsweise teuren – Stück Hardware für SMS- und Sprachkommunikation einbinden. Letzteres kann allerdings dazu führen, dass AktivistInnen Ärger mit ihren lokalen Telekommunikationsanbietern bekommen, was in Krisengebieten aber wohl niemanden ernstlich interessieren dürfte.

Wie genau „Commotion Wireless“ in der Praxis funktionieren wird, ist noch nicht ganz klar – die MacherInnen peilen einen Starttermin für Anfang 2013 an und bitten externe EntwicklerInnen um Mithilfe. Anleitungen und Handbücher müssen geschrieben und in möglichst viele Sprachen übersetzt werden, damit das Projekt auch wirklich weltweit genutzt werden kann. Windows, Mac, GNU/Linux, WLAN-Router-Plattformen wie OpenWrt und Smartphone- und Tablet-Betriebssysteme wie Android sollen damit unterstützt werden – eventuell auch

Apples iPhone. Die MacherInnen versprechen, dass man ihr Netz möglichst anonym und sicher nutzen können wird: So soll etwa nicht mit nachverfolgbaren IP-Adressen gearbeitet werden; die Kommunikation zwischen Knoten erfolge stets verschlüsselt.

Dass „Commotion Wireless" infiltriert wird, lässt sich allerdings nicht völlig ausschließen: Sollte sich eine Regierung entschließen, einen eigenen Knoten im Netz anzubieten, könnten zumindest Daten, die direkt an diesen Knoten gehen, entschlüsselt und gelesen werden. Anderer Datenverkehr, der den Regierungsknoten nur zur Weiterleitung nutzt, wäre davon allerdings nicht betroffen. Die Gefahr, dass gelauscht wird, sei so geringer als im offenen Internet. Allerdings bestehe stets die Gefahr, dass jemand versuchen könne, das „richtige" Mesh-Netzwerk nachzuahmen, weshalb man jedes neue Netz zunächst misstrauisch prüfen sollte. Hier hilft ein zusätzlich verschlüsselter Datenverkehr – etwa für E-Mails zwischen Knoten. Letztlich soll innerhalb von „Commotion Wireless" alles möglich sein, was auch im regulären Internet geht – vom Dateitransfer bis zum VoIP-Telefonat. Die Anbindung an den Rest der Welt könnten Aktivisten dann z. B. in einem angrenzenden Land herstellen, in dem das Netz nicht zensiert wird – dazu würde dann das WLAN-Signal vom letzten inländischen Knoten gen Ausland gesendet. Wen stört, dass die US-Regierung das Projekt mitfinanziert, sollte Vertrauen daraus schöpfen, dass „Commotion Wireless" ein quelloffenes Vorhaben ist – der gesamte Code wird im Netz nachlesbar sein (Schwan www.taz.de 27.06.2012).

USA

Klout: Personenscoring in sozialen Netzwerken

Das in San Francisco residierende Unternehmen Klout (inspiriert vom englischen „clout" = Einfluss, Macht) verspricht sich vom Personenscoring auf der Basis von Internetdaten einen Marketing-Goldrausch. Joe Fernandez, einer der Gründer des Who´s who des Internet erläuterte sein Angebot: „Wir bewerten, wie effektiv jemand soziale Netzwerke nutzt und andere damit beeinflusst". In Konkurrenz zu Start-ups wie Kred oder PeerIndex wird gemessen, wie erfolgreich Internetnutzende twittern oder sich bei Facebook engagieren. Internetexperte Mark Schaefer kommentierte: „Wer auf Facebook, LinkedIn oder Twitter aktiv ist, kann davon ausgehen, dass er taxiert wird." Die ersten 2000 Klout-Scores berechnete der Oxford-Studienabbrecher Fernandez im Jahr 2007 noch in einer einfachen Excell-Tabelle. Inzwischen erfolgt die Bewertung vollautomatisch. Mit einer streng geheim gehaltenen Berechnungsformel, die dauernd weiterentwickelt wird, wird analysiert, wieviel Texte ein Twitter-Nutzender ins Netz stellt, wie oft die Tweets weitergeschickt werden, wer welche Facebook-Einträge kommentiert... Teenieschwarm Justin Bieber ist der einzige, der den Höchstwert von 100 schaffte. Barack Obama wurde mit 94, Bill Gates mit 75 taxiert. Beispiele für deutsche Internetbewertete (Stand 26.07.2012): Peter Altmeier, CDU, 63; Sigmar Gabriel, SPD, 58; Dorothee Bär, CSU, 54; Jürgen Trittin, Grüne, 52; Petra Pau, Linke, 44; Philipp Rösler, FDP, 39.

Zusätzlich ordnet der Dienst den Nutzenden Themen zu, über die sie oft twittern. Den erfolgreichsten NetzbürgerInnen – bei Klout u. a. „Taste Maker" genannt - winken Gutscheine für Massagen, Kosmetika, Hotel-Upgrades... Die Fluggesellschaft Virgin America spendierte im Jahr 2011 120 Freiflüge für ihre neue Toronto-Verbindung. Im Sommer 2012 konnten 2000-Klout-Nutzende mehrere Tage lang das Elektroauto „Volt" von Chevrolet testen. Über 300 Firmen hat Klout für derartige Werbeaktionen gewinnen können. Mit dem Umschmeicheln der vermeintlichen Netzelite soll Gratiswerbung erreicht werden, indem die unermüdlich twitternden Beglückten ihr Glück tausendfach in die Internet-Welt hinausposaunen. Fernandez: „Die Firmen realisieren, dass es besser ist, ihre Produkte in die Hand einflussreicher Leute im Netz zu geben, als sie auf Werbetafeln oder im Fernsehen zu zeigen." Tweet-zu-Tweet-Propaganda sei zudem weit billiger als Werbung mit teuren Hollywood- und Sportstars.

Jaron Lanier kritisierte: „Das Leben der Leute wird mehr und mehr von dummen Algorithmen bestimmt". Tatsächlich gewinnen die Zahlen, deren Zustandekommen völlig undurchsichtig ist, an praktischer Bedeutung. So meinte Alex Salkever, Produktmanager des Telekommunikationsunternehmens Telefónica: „Ich bin nicht immer mit den Wertungen solcher Dienste einverstanden, aber ich ignoriere sie nie." Schaefer berichtete von dem Fall eines Marketingexperten mit 15 Jahren Berufserfahrung, der eine Stelle nur deshalb nicht bekam, weil sein Klout-Score zu niedrig war. Da der Score praktische Bedeutung z. B. in Bewerbungsverfahren hat, wenden sich viele Menschen an das Unternehmen, die ihren Score verbessern wollen. Fernandez: „Wir ordnen jedem Gesicht eine Nummer zu, natürlich kann das am Ego kratzen." Ein neuer Algorithmus soll künftig den Einfluss der UserInnen in der realen Welt mit berücksichtigen. Da der Algorithmus aber dumm ist, passiert es, dass z. B. der Londoner Big Ben mit 75 auf einem der vorderen Ränge bei Klout rangiert, weil ein inoffizielles Twitterkonto von ihm stündlich die Glockenschläge versendet. Bei Klout hat es Big Ben so zum Experten für „Tee" und „Drogen" gebracht (Bethge Der Spiegel 31/2012, 98).

Kanada

Audio- und Vidoüberwachung bei Flughafenkontrollen

In Kanada sollen die Sicherheitseinrichtungen an Flughäfen massiv verstärkt werden. Neben hochauflösenden Kameras sollen dazu auch Abhörmikrofone eingesetzt werden, um Passagiere und Personal zu überwachen. In Ottawa und Halifax ist nach Presseberichten die Technologie schon installiert, wird allerdings noch nicht eingesetzt. Ein Sprecher der Grenzbehörde CBSA teilte mit: „Derzeit werden keine Tonaufnahmen gemacht, das wird zu einem späteren Zeitpunkt in Betrieb genommen." Die Gespräche zwischen Sicherheitsbeamten und Passagieren sollen aufgezeichnet werden, jedoch keine

Privatgespräche. Hauptsächlich gehe es darum, gegen Schmuggler vorzugehen, sagte Vic Toews, Minister für öffentliche Sicherheit. Die stehen im Verdacht, Flughafenmitarbeitende zu bestechen, um illegal Waren über die Grenze zu bringen. Nach 30 Tagen sollen die Audio- und Videodaten wieder gelöscht werden. Die für Flughafenangestellten in Ottawa zuständige Gewerkschaft teilte mit, sie befürchte, dass Informationen aus den Audiodaten künftig in den Mitarbeiterakten auftauchen könnten. Toews kündigte an, dass jedoch zunächst ein Datenschutzgutachten erstellt werden müsse, bevor solche Technologie eingesetzt wird.

Ann Cavoukian, Datenschutzbeauftragte der Provinz Ontario, kündigte an, gegen diesen Lauschangriff vorzugehen. Im Forum von „CBS" hagelt es zudem empörte Kommentare von LeserInnen, z. B. schrieb einer: „Wir verwandeln uns mehr und mehr in einen totalitären Staat." Vergleiche mit George Orwells Roman „1984" wurden gezogen. Ein anderer Leser meinte: „Ich kann mir schon vorstellen, wie sinnvoll das ist, da bekanntlich die meisten Terroristen am Flughafen über ihre Pläne sprechen" (www.spiegel.de 21.06.2012).

Israel

DNA-Datenbank zwecks Zuordnung von Hundekot

Jerusalems Stadtverwaltung hat dem Hundekot den Kampf angesagt und den Aufbau einer Datenbank mit der DNA aller Jerusalemer Vierbeiner angekündigt. Damit soll gefundener Kot auf Gehwegen, Parkwiesen und Spielplätzen zu Hund und Halter zurückgeführt werden, um daraufhin Strafen verhängen zu können. Der DNA-Test erfolgt als Speichelprobe mit einem Wattestäbchen. Gemäß einer Anordnung können HundehalterInnen im Notfall vorgeladen werden. Gemäß der Planung werden alle ca. 11.000 in Jerusalem registrierten Hunde ab Anfang 2013 erfasst. Stadt-Veterinär Zohar Dvorkin: „Wenn wir 70 bis 80% der registrierten Hunde in der Datenbank haben, können wir damit anfangen, die Fäkalien einzusammeln". Ein DNA-Test wird umgerechnet 30 Euro kosten. Die Refinanzierung soll über Strafgebühren in Höhe von 150 Euro erfolgen. Nicht registrierte Hunde können weiterhin ungestraft koten. Dvorkin beteuert, dass es nicht ums Geld geht. Er sei zufrieden, wenn die Hundebesitzer den Kot ihrer Tiere künftig selbst wegräumen. Ein ähnliches Projekt in der Tel Aviver Vorstadt Petach Tikwa war 2008 von der New York Times zu einer der „besten Ideen des Jahres" gekürt worden, aber letztlich daran gescheitert, dass die Hundebesitzer nicht zur Abgabe einer Speichelprobe ihrer Tiere gezwungen werden konnten (Münch SZ 13.06.2012, 10).

Afghanistan

Militärische und zivile Luftüberwachung mit Ballonen

Das US-Militär setzt bei seinen Sicherheitsmaßnahmen in Afghanistan zunehmend Kontroll- und Überwachungstechnologie ein. Dazu gehören „Aerostat" genannte Helium-Ballons, die zumeist in mehr als 450 Meter Höhe und mit einer Größe von 35 oder 23 Metern über Kabul oder Kandahar schweben und mit Infraraot- und Videokameras ausgestattet sind. Im Zhare-Distrikt der Provinz Kandahar, einem Schwerpunkt der US-Truppenkonzentration im Jahr 2010, ist praktisch von jedem Dorf aus ein solcher Ballon in Sichtweite. Die Ballons wurden Teil eines immer breiter werdenden Spektrums von Kontrolltechnologie, zu der auch Drohnen, Überwachungstürme auf Militärbasen und Videonetzwerke in Kabuls Straßen gehören, mit denen amerikanische wie afghanische Kräfte ein Auge auf gefährdete und umkämpfte Gebiete halten. Mit dem Videonetzwerk werden z. B. Straßenkreuzungen, der oberste Gerichtshof und an Militärlagern vorbeiführende Straßen kontrolliert.

Die Ballons werden von vielen Afghanen achselzuckend hingenommen. Aber anderen ist die dauernde Überwachung bewusst, wie dem 18jährigen Mir Akbar: „Das beobachtet uns Tag und Nacht". Ein Bewohner von Asadabad, der Hauptstadt der Provinz Kunar, wo Familien oft während der Sommerhitze auf ihren Dachterrassen schlafen, meint: „Wir können nicht mehr auf unseren Dächern schlafen". Manche halten es für unmoralisch, dass Frauen und Kinder auch in Hinterhöfen von Ausländern auf den Bildschirmen beobachtet werden.

Die Helium-Ballons wurden von den USA erstmals 2004 im Irak verwendet und werden seit 2007 in Afghanistan eingesetzt. Sie haben gegenüber den teuren Drohnen, die viel mehr Aufmerksamkeit auf sich ziehen, Vorzüge. Ray Gutierrez, der an dieser Überwachungstechnologie ausbildet, meint: „Wir können Kampfgebiete in einer Art einsehen, wie dies uns vorher nie möglich war." Die Taliban-Kämpfer fürchten die Luftschiffe und versuchen die Gegenden unter ihnen zu vermeiden oder sich dort als Bauern zu verkleiden. Nach Ansicht des US-Militärs haben sich mit dieser Luftüberwachung die Angriffe aus dem Hinterhalt verringert. Sommerwinde und Stürme führen ab und zu dazu, dass die Halteseile reißen. Wenn die Ballons zum Zweck der Sicherung oder der Überholung heruntergeholt werden, haben sie regelmäßig viele Schußlöcher. Es bedarf aber, so der Instandsetzer Eddy Hogan, vieler hunderter Patronen, um einen Ballon vom Himmel zu holen (Graham Bowley, The New York Times, selected for Süddeutsche Zeitung, 21.05.2012, 3).

Japan

Beamte müssen per Fragebogen Tatoos offenlegen

Die ca. 33.000 Beamten in Osaka mussten auf Anweisung von Bürgermeister Toru Hashimoto eine Anfrage ihrer Personalreferate beantworten, wieviel Tätowierungen sie auf welchen Körperteilen in welcher Größe tragen und ob sie sich die Tatoos vor Eintritt in den Beamtenstand stechen ließen. Tatoos im Intimbereich wurden nicht als meldepflichtig eingestuft; eine freiwillige Bekenntnis wurde dennoch erwartet. 110 Beamte ließen so ihre Tatoos registrieren; 513 füllten den Fragebogen nicht aus. Der Bürgermeister drohte daraufhin mit Gehaltskürzung, wenn nicht innerhalb einer weiteren Woche der

Fragebogen ausgefüllt wird: „Unseren Bürgern ist es unangenehm, wenn sie von einem Beamten mit Tätowierungen bedient werden. Das untergräbt ihr Vertrauen in die Stadt.“ Beamte mit sichtbaren Tatoos sollen versetzt werden, damit sie keinen Bürgerkontakt mehr haben: „Wenn sie ein Tatoo wollen, können sie in der Privatwirtschaft arbeiten. Die Modebranche nimmt sie vielleicht.“

Auslöser der Aktion war, dass im Februar 2012 ein Angestellter einer Kinderkrippe den Kleinen sein Tatoo auf dem Arm gezeigt habe, was diese angeblich verstörte. Tätowierungen sind in Japan tabu und gelten als Zeichen der Yakuza, der japanischen Mafia. Bis ins 17. Jahrhundert waren Tatoos salonfähig; seither werden sie nur noch in der Uyiko, der Welt der Schauspieler, Sumo-Ringer, Geishas, Prostituierten und Geschäftsmacher toleriert. Von 1868 bis zum Ende des zweiten Weltkriegs hatte die Regierung alle Tatoos verboten. Die meisten Onsen, Japans Thermalbäder, verweigern bis heute Tätowierten den Eintritt. Jugendliche lassen sich dennoch oft vom Tätowieren nicht abhalten.

Bürgermeister Hashimoto war als Fernsehanwalt bekannt geworden und versucht derzeit die Politik aufzumischen und hat für die nächsten Parlamentswahlen eine nationale, völlig auf seine Person ausgerichtete Partei aufgebaut. Der Populist, kurz nach Fukoshima noch für die Atomkraft, lehnt inzwischen das Wiederanfahren von Atomreaktoren ab. Er lässt Lehrer bestrafen, die bei Schulfeiern die Nationalhymne aus der militaristischen Zeit nicht mitsingen. Hashimoto will durchsetzen, dass seine Beamten in Osaka mit bis zu zwei Jahren Gefängnis bestraft werden, wenn sie an Demonstrationen teilnehmen oder Flugblätter verteilen. Von Beamten wird in Japan generell erwartet, dass sie sich nicht politisch betätigen (Neidhart SZ 26.-28.05.2012, 1).

China

Ai Weiwei lädt Polizei zu sich nach Hause ein

Der regimekritische Künstler Ai Weiwei aus China hat im Juni 2012 Polizisten eingeladen, bei ihm im Büro zu arbeiten. Er habe ihnen gesagt: „Dass ihr mich ständig ausspioniert, ist völlig ineffizient. So bekommt ihr doch gar nicht all die Informationen, die ihr wollt, oder ihr zieht daraus falsche Schlüsse. Also zieht doch bei mir ein“. Die Beamten haben jedoch abgelehnt.

Dies ist nicht die erste offensive Selbstverteidigung von Weiwei gegen die 15 Überwachungskameras rund um sein Haus, mit denen er und seine BesucherInnen gefilmt werden, und dem dauernd vor dem Haus stehenden Polizeiauto. April 2012 installierte Weiwei 4 Webkameras, die sein Leben für alle Welt ins Netz übertrugen. Weiweicam.com brachte 5,2 Millionen Klicks in 46 Stunden. Dann befahlen die Behörden, die Seite abzuschalten. Weiwei gehochte.

Genau ein Jahr zuvor, am 03.04.2011, war er verhaftet und 81 Tage eingesperrt worden. Dabei wurde er immer wieder verhört, so er selbst: „zwei Drittel Schikane, ein Drittel Gehirnwäsche.“ Offiziell findet gegen ihn ein Verfahren wegen angeblicher Steuerhinterziehung statt. Im Juni 2012 kam ein Dokumentarfilm über den Künstler in die westlichen Kinos, der die Eskalation in einem Portrait bis zur Festnahme nachzeichnet. „Ai Weiwei: Never Sorry“ ist ein Film über Chinas kafkaesken Polizeistaat und über Männer mit Überwachungskameras, die plötzlich selbst gefilmt werden. US-Regisseurin Alison Klayman hatte den Künstler drei Jahre immer wieder mit der Kamera begleitet. Weiwei erstattete 2012 auf einer chinesischen Polizeiwache Anzeige wegen einer Prügelattacke chinesischer Polizisten gegen ihn im Jahr 2009, weshalb er später wegen einer lebensbedrohlichen Hirnblutung operiert werden musste. Bei der Aufnahme der Anzeige wurde der Polizist durch einen Assistenten des US-Kamerateams gefilmt, der das Formular ausfüllen musste. Dessen Blick verrät eine Supermacht in Panik, so das Nachrichtenmagazin „Der Spiegel“.

Am 20.06.2012 fand eine gerichtliche Anhörung zu den Vorwürfen gegen Weiwei statt. Ihm war aber untersagt worden, sein Haus zu verlassen. An der Anhörung nahme Weiweis Ehefrau Lu Qing gemeinsam mit mehreren Anwälten und einem Buchhalter teil. Filmaufnahmen waren selbst vor dem Gerichtsgebäude verboten (SZ 06./07.06.2012, 11; Wolf Der Spiegel 24/2012, 135; SZ 21.06.2012, 8).

Technik-Nachrichten

Trojaner „Gauss“ infiziert Rechner vor allem im Nahen Osten

Bei seinen Untersuchungen zum 20-MByte-Trojaner „Flame“ sind die Sicherheitsforscher von Kaspersky Lab auf einen wesentlich weiter verbreiteten Trojaner, der „Gauss“ bezeichnet wird, gestoßen, der vermutlich Zehntausende Rechner insbesondere im Libanon, in Israel und Palästina infiziert hat. Zu seinen Schadfunktionen gehört der Diebstahl von Internet-Kennwörtern, Zugängen zu Online-Konten, persönlichen Cookies, des Browser-Verlaufs und anderen individuellen Systemeinstellungen. Der Name „Gauss“ stammt aus dem Hauptmodul des Schädlings; auch andere Module sind nach berühmten Mathematikern benannt.

Über welche Sicherheitslücke Gauss sich Zugang zu den Zielsystemen verschaffte, blieb zunächst unklar. Die Weiterverbreitung erfolgt über USB-Sticks. Dabei nutzt der Trojaner dieselbe Sicherheitslücke bei der Behandlung von .LNK-Dateien wie zuvor Flame

und Stuxnet. Gauss legt die erspähten Informationen in einer versteckten Datei auf dem Stick ab. Gemäß Chef-Analyst Magnus Kalkuhl ähnelt Gauss dem Riesentrojaner Flame sowohl im Aufbau als auch in der Struktur der Module, der Code-Basis sowie in der Art, wie der Trojaner Kontakt zu den Fernsteuerungs-Servern aufnahm. Dies legt einen gemeinsamen Urheber nahe – Flame und Stuxnet werden den Geheimdiensten von Israel und den USA zugeschrieben. Insofern ist erstaunlich, dass die Spionagefunktionen von Gauss auch den Online-Zugriff auf Bankkonten umfassten. Kaspersky zufolge sucht der Trojaner konkret nach Kundendaten für die Bank of Beirut, Banque Libano-Française (EBLF), Blom Bank, Byblos Bank, Credit Libanais und Fransabank. Der Trojaner soll auch Zugriffe auf Konten bei Citibank und PayPal abhören.

Gauss wurde von Kaspersky erstmals im September 2011 gesichtet und im Juni 2012 als Trojan-Spy.Win32.Gauss identifiziert. Dies blieb den Urhebern des Trojaners nicht lange verborgen: Im Juli 2012 wurden die Steuerungs-Server deaktiviert; bei infizierten Systemen befindet sich der Trojaner seitdem in einem Schlafmodus. Kasperskys Sicherheitsnetzwerk zählte seit Mai 2012 etwa 2.500 Infektionen – dies sind allerdings nur Funde auf Rechnern mit installierten Kaspersky-Produkten. Bei Flame hatte Kaspersky 700 Infektionen gezählt. Wie Duqu und Flame enthält auch Gauss einen Selbstzerstörungsmechanismus – nach 30 Aufrufen von einem USB-Stick aus löscht Gauss sich selbstständig, um einer Erkennung durch Virenschutzprogramme zu entgehen (SZ 10.08.2012, 23; www.heise.de 09.08.2012).

Forschergruppe deckt Kfz-Sicherheitsschwachstellen auf

Da Autos zunehmend für Hacker interessant werden, haben Forschende des Centers for Automotive Embedded Systems Security (CAESS) das Auto systematisch nach Schwachstellen abgesucht - angefangen über die Werkstatt-Schnittstelle zur Motorelektronik über eine versteckte serielle Schnittstelle im Radio bis hin zu Bluetooth und Mobilfunk. Die Technology Review berichtet in ihrer Ausgabe 08/2012, dass es den Forschenden u. a. gelang, per Telefon die Telematik-Einheit des Autos anzurufen, dem Software-Modem eine bestimmte Tonfolge vorzuspielen und so einen Puffer-Überlauf zu provozieren. Anschließend konnten sie aus der Ferne die Fahrzeugelektronik manipulieren. Einmal in die Fahrzeugelektronik eingedrungen, konnten sie unter anderem die Türen öffnen oder die Wegfahrsperre abschalten. Selbst die Bremsen ließen sich auf diese Weise deaktivieren. Franziska Rösner, die als Doktorandin am CAESS-Hack mitgearbeitet hat, erläuterte: „Es war tatsächlich die normale Fahrzeugbremse, die man während unserer Versuche mit dem Bremspedal nicht mehr kontrollieren konnte“. Die gehackten Fahrzeuge wurden dazu gebracht, laufend ihre Position zu melden und das Mikrofon der Freisprecheinrichtung einzuschalten. Auf diese Weise konnten Forschende in San Diego vom Schreibtisch aus ihre KollegInnen im 2.000 Kilometer entfernten Seattle während einer Autofahrt belauschen.

Mit den erprobten Angriffen ließen sich potenziell lebensgefährliche Unfälle provozieren. Unmittelbare Gefahr für Leib und Leben erwartet die CAESS-Arbeitsgruppe durch die von ihnen aufgedeckten Schwachstellen derzeit nicht, so der Leiter Tadayoshi Kohno: „Meine Kollegen und ich fahren unsere Autos weiterhin entspannt“. Zehn Forschende mussten immerhin zwei Jahre lang herumtüfteln, um die geschilderten Lücken zu finden. Mit ihrer Aktion wollen sie Autohersteller für die Probleme sensibilisieren. Franziska Rösner: „Was uns Sorgen macht, ist, dass Autos nun zunehmend ans Internet angeschlossen werden. Wenn man nicht von Anfang an für Sicherheit sorgt, wird es hinterher gefährlich“ (SZ 06.08.2012, 37; www.heise.de 27.07.2012).

Indoor-Navigation als Orientierungshilfe in und zwischen Gebäuden

Das Fraunhofer-Institut für Photonische Mikrosysteme (IPMS) in Dresden hat ein Navigationssystem für Smartphones entwickelt, das MitarbeiterInnen, KundInnen oder Lieferanten den Weg durch das Labyrinth großer Gebäudekomplexe weist - im Inneren wie auch im Außenbereich. Mit „2D-GN“ wird die zweidimensionale Gebäudenavigation möglich, um den Menschen z. B. in großen medizinischen Einrichtungen wie Krankenhäusern oder Reha-Kliniken, aber auch in Flughäfen oder Möbelhäusern mit unzähligen Gebäuden, Gängen und Räumen die Orientierung zu erleichtern. Hans-Jürgen Holland vom IPMS: „Wir haben größten Wert auf einfache und unkomplizierte Handhabung gelegt.“ Der Fokus habe insbesondere auf den „60 plus“ gelegen und auf der Situation von Menschen jeden Alters, die zum Zeitpunkt der Suche in Termindruck, Hektik oder Stress und dadurch emotional abgelenkt sind. Das System soll analoge Beschilderung und strukturierte Architektur nicht ersetzen, aber ergänzen. Grundlage von 2D-GN sind exakte Gebäudepläne und die Lokalisierung der navigierenden Person. Nach Auswahl des Ziels werden die eigene Position und der errechnete Weg auf einem Smartphone angezeigt und vergleichbar mit der Kfz-Navigation dauernd aktualisiert.

Zur Lokalisierung wird im Außenbereich die Satellitennavigation GPS verwendet. Wenn Nutzende ein Haus betreten, schaltet das System auf Indoor-Navigation um. Die Position des Smartphones und seines Nutzenden wird mit Hilfe eines WLAN-Netzes bestimmt. Es bedarf mehrerer Hotspots, über die jederzeit jeder Ort in den Gebäuden erreicht und bestimmt werden kann. Holland: „Für sicherheitsrelevante Bereiche lässt sich das System durch eine Ortung aller Personen, die es nutzen, erweitern. Diese Informationen laufen auf einem PC ein und können so der Überwachung aller Personen in diesem Gebiet dienen.“ Das 2D-GN kann mit Sensoren für Gas, Rauch, Wärme usw. ausgestattet werden, so dass die Nutzenden und die Zentrale in Gefahrensituationen informiert werden können. Für medizinische und andere Servicebereiche gibt es eine andere Zusatzfunktion, so Holland: „Über die Geräte können auch Informationen wie Sprechzeiten übermittelt werden. In Reha-Einrichtungen

lässt sich das ganze Tagesprogramm mit Erinnerungsfunktion hinterlegen." Google hat ein vergleichbares System entwickelt, das zunächst in den USA und in Japan zum Einsatz kommen soll. Diplompsychologe Riklef Rambow, Professor für Architekturkommunikation am Karlsruher Institut für Technologie, erläutert Nutzen und Gefahren: „Damit wird das Navi zur Kundenlenkung genutzt, eine Entwicklung, die mobil fortsetzt, was bei Internetkäufen am PC seit Jahren ausgebaut wird. So generiert die kostenträchtige Infrastruktur des Navis den Betreibern Gewinne. Auf der anderen Seite sollten Kunden sich fragen, wie gläsern sie sich machen wollen" (Klaasen SZ 20.07.2012 S. V2/2).

Menschen können Alter am Geruch bestimmen

Ein Experiment von US-amerikanischen Forschenden zeigte, dass ähnlich wie viele Tiere auch der Mensch die Fähigkeit besitzt, die unterschwelligen chemischen Signale des Alterns wahrzunehmen und so per Geruch das ungefähre Alter eines Gegenübers zu bestimmen. Bei dem Experiment konnten Testpersonen Proben von Achselschweiß nur anhand ihres Geruchs korrekt der Altersgruppe zuordnen. Für die Studie schliefen Geruchsspendende aus drei Altersklassen fünf Nächte lang in einem T-Shirt mit einem schweißabsorbierenden Stoffläppchen unter den Achseln: 20 bis 30, 45 bis 55 und 75 bis 95 Jahre alt. Alle Läppchen mit Geruchsproben wurden zerkleinert und jeweils einzeln in luftdichte Glasgefäße gelegt. Als TestschnüfflerInnen dienten 41 junge Männer und Frauen, die in mehreren Durchgängen jeweils an zwei Behältern mit unterschiedlichen Proben rochen. Bei jedem Probenpaar sollten sie angeben, welcher Altersklasse sie die jeweiligen Spendenden zuordnen würden und wie intensiv und unangenehm sie den Geruch empfanden. Wie das Forscherteam berichtet, lagen die Testpersonen bei ihrer Alterseinschätzung häufig richtig. Die wenigsten Fehler seien ihnen bei der Zuordnung des Geruchs der alten Menschen unterlaufen. Gemäß der Publikation im Fachmagazin „PloS ONE" rochen die Senioren aber nicht etwa stärker. Vielmehr empfanden die jungen Probanden den Achselschweiß der Älteren sogar als weniger intensiv und angenehmer als den Körpergeruch von jungen und mittelalten Menschen.

Schon seit längerem ist bekannt, dass der menschliche Körpergeruch eine Vielzahl chemischer Substanzen enthält, die bestimmte Informationen transportieren. Studienleiter Johan Lundström vom Monell Chemical Senses Center in Philadelphia erläuterte: „Der Mensch kann Signale im Körpergeruch wahrnehmen, die es uns erlauben, beispielsweise Krankheiten zu erkennen, einen passenden Partner zu finden und Verwandte von Nichtverwandten zu unterscheiden." Die Wahrnehmung dieser Signale geschehe allerdings meist unbewusst und unterschwellig. Studien mit Tieren haben bereits gezeigt, dass sich deren Körpergeruch im Laufe des Lebens verändert. Forschende vermuten, dass dies den Männchen dabei hilft, beispielsweise bei der Partnerwahl ältere, nicht mehr so fruchtbare Weibchen zu erkennen und zu meiden. Weibchen wiederum identifizieren über den Geruch Männchen, die älter sind und damit erfolgreich über längere Zeit überlebt haben. Ihre Nachkommen könnten daher von den guten Genen dieses Männchen profitieren. Dass auch Menschen die Fähigkeit der Alterserkennung am Geruch besitzen, zeigt nun das Experiment der Monell-Forschenden. Welche der zahllosen Einzelsubstanzen im Körpergeruch die Information über das Alter vermitteln, ist noch unklar. Im nächsten Schritt sollen diese Biomarker identifiziert werden. Weitere Tests sollen zeigen, wie das menschliche Gehirn diese chemischen Informationen verarbeitet und bewertet (http://lifestyle.t-online.de 31.05.2012; SZ 31.05.2012, 24).

Genetische Pränataldiagnostik mit Mutterblut und Vaterspeichel

Genetik-Forschende der University of Washington/USA haben erstmals das gesamte Erbgut eines ungeborenen Kindes entziffert, indem sie das Blut der Mutter und den Speichel des Vaters analysierten (Science Translational Medizine, online). Schon in der 18. Schwangerschaftswoche können werdende Eltern so künftig Auskunft über genetische Auffälligkeiten ihres Nachwuchses erhalten - nicht nur über das Down-Syndrom, sondern über jedwede Erbkrankheit sowie Mutation. Die Erbanlagen des Kindes so zu ermitteln ist möglich, weil sich im mütterlichen Blut DNA des Ungeborenen findet. Mit modernen Methoden lässt sich diese isolieren und entziffern. Weil aber das Erbgut in kleine Schnipsel zerstückelt ist, brauchen die Forschenden auch noch das Erbgut von Mutter und Vater. Am Computer setzen sie dann das wahrscheinliche Erbgut des Kindes zusammen. Als sie ihr Ergebnis nach der Geburt des Babys verglichen, lag die Übereinstimmung bei 98%. Sie hatten 39 der 44 Neu-Mutationen korrekt vorhergesagt, die bei dem Kind sich eigenständig entwickelt hatten. Einer der Forscher, Jacob Kitzmann kommentierte: „Früher konnte man sehen, dass zwei Bücher zusammengefügt wurden. Jetzt können wir ein einziges Wort, das in beiden Büchern falsch buchstabiert ist, erkennen." Die Arbeit eröffne die Möglichkeit, „das ganze Genom des Fötus auf mehr als 3.000 monogenetische Erkrankungen zu scannen", so Teamleiter Jay Shendure. Die Krankheiten seien selten, aber zusammen beträfen sie etwa 1% der Neugeborenen. Es gehe dabei nicht um Abtreibung. Wenn Leiden frühzeitig entdeckt werden, mache dies in vielen Fällen medizinische Hilfe möglich. Das Experiment wurde mit einem zweiten Paar sogar in der 9. Schwangerschaftswoche mit ähnlichem Erfolg wiederholt. Ein solch früher Zeitpunkt bereitet EthikerInnen Sorgen, weil z. B. in Deutschland eine Abtreibung bis zur 14. Schwangerschaftswoche straffrei ist. Jede unerwünschte genetische Information könnte eine Frau dazu bewegen, sich für den Abbruch zu entscheiden.

Das Konstanzer Diagnostikunternehmen LifeCodexx wollte ab Juli 2012 einen Test anbieten, der schon aus dem Blut der Schwangeren ermitteln kann, ob beim Fötus das Chromosom 21 dreimal statt zweimal vorkommt und er somit eine Trisomie 21 hat, also ein Down-Syndrom. Der Bluttest auf Down-Syndrom kommt dann in 20 deutschen Pränatalzentren und Frauenarztpraxen zum Einsatz, mit denen LifeCodexx zusammenar-

beit. Die Untersuchung kostet 1.250 Euro, die die Schwangere selbst zahlen muss. Von der Blutabnahme bis zum Testergebnis dauert es etwa 2 Wochen. LifeCodexx vermutet, dass ihr Test 600 bis 700 ungeborene Kinder pro Jahr „vor den Folgen eines tödlichen Eingriffs bewahren“. Die Deutsche Gesellschaft für Gynäkologie schätzt niedriger und berechnete statistisch, dass ca. 150 Kinder durch die Fruchtwasseruntersuchung und Chorionzottenbiopsien jährlich in Deutschland sterben, auch wenn sie gesund sind. Zehntausende Schwangere lassen die Prozedur über sich ergehen, bei der PränatalmedizinerInnen mit einer langen Spezialnadel durch die Bauchdecke stechen und nah am Fötus Zellen entnehmen, was in mindestens jedem 200. Fall eine Fehlgeburt auslöst.

Der Bonner Humangenetiker Peter Propping stellt den Sinn in Frage, das ganze Genom des Fötus zu sequenzieren. Die meisten Mutationen im menschlichen Erbgut machten nichts aus: „Wir alle tragen zahlreiche Neu-Mutationen, ohne dass das Konsequenzen hätte.“ Viele weitere Veränderungen erhöhten das Risiko für Krankheiten nur - meist um wenige Prozent. Der Erlanger Theologe Peter Dabrock, stellvertretender Vorsitzender des Deutschen Ethikrates: „Wir müssen wegkommen von dieser genzentrierten Sicht.“ Die Information, ein Ungeborenes habe zum Beispiel ein um 5% erhöhtes Alzheimerrisiko, sei wertlos. Je tiefer das Verständnis der menschlichen Genetik reiche, desto klarer werde, dass eine Genomanalyse nur wenige zuverlässige Aussagen über das Schicksal eines Menschen erlaube.

Für schwerwiegende Mutationen existiert bereit ein Bluttest, der mehr als 1.200 monogenetische Erbkrankheiten erkennen kann. Stephen Kingsmore vom National Center for Genome Resources in Santa Fe/USA hat diesen Test nicht zum Screening von Föten konzipiert, sondern für junge Erwachsene. So können Partner das Risiko ermessen, ob sie beide - bislang unerkannt - Träger desselben Erbleidens sind. Jeder Mensch trägt bis zu 60 krankhaft veränderte Gene. Folgen hat das allenfalls, wenn die PartnerIn denselben Defekt hat. Dann beträgt die Wahrscheinlichkeit, dass bei dem Kind die jeweilige Krankheit ausbricht, ein Viertel. In den USA wird dieser Test auf Wunsch schon angeboten. Propping spricht sich dafür aus, unbedingt die psychosozialen Folgen eines solchen Anwendung zu untersuchen: „Was machen Eltern mit solchen Informationen?“ Sich scheiden lassen, Kinder erst in der Petrischale zeugen und dann die ohne Mutation auswählen oder doch der Natur ihren Lauf lassen?

Die neue Analysemethode ist heute noch teuer und kompliziert. Schätzungen liegen bei bis zu 50.000 Dollar pro Untersuchung. Die Preise werden aber voraussichtlich schnell sinken. Die Sequenzierung eines Genom kostete im Jahr 2001 ca. 100 Mio. Euro; heute entstehen nur noch Kosten von weniger als 10.000 Euro. Elke Holinski-Feder äußerte Befürchtungen hinsichtlich der freien Entscheidung der werdenden Eltern: „Die Eltern werden nicht mehr ein noch aus wissen. Es wird keine zehn Jahre mehr dauern, bis alle Eltern vor der Frage stehen: ´Lasse ich das machen?´“. Die Eltern erhielten dann eine Unzahl genetischer Informationen, mit denen selbst HumangenetikerInnen bislang oft nichts oder nur wenig anfangen können. Holinki-Feder schlägt als Weg aus dem Kontrolle-Abbruch-Dilemma vor, dass Paare, die sich unbedingt testen lassen wollen, dies vor einer Schwangerschaft tun. Bei beiden Partnern könne nach Veränderungen in den knapp 500 bekannten Genen gesucht werden, die, wenn sie unglücklich zusammentreffen, bei einem Kind zu schwerster Krankheit und Behinderung führen können: „Das wird heute schon in manchen Fällen gemacht und kann mitunter viel Leid ersparen“ (Berndt SZ 08.06.2012, 16; Nieder SZ 15.06.2012, 18; von Bredow, Hackenbroch Der Spiegel 24/2012, 126 f.).

Textilien mit Geruchssensoren

Die Firma Peratech aus Großbritannien hat ein Sensormaterial entwickelt, das sich als „elektronische Nase“ in Kleidung integrieren lässt. Mit der Technik werden flüchtige organische Verbindungen, sogenannte VOCs, detektiert. VOCs können aus den unterschiedlichsten Quellen stammen und auf schädliche Chemikalien in der Umwelt hindeuten – oder ein Hinweis darauf sein, dass mit dem Körper etwas nicht stimmt. Viele VOCs sind nahezu geruchlos und nur in geringsten Spuren vorhanden. Schon seit Langem versuchen Forschende, tragbare und besonders empfindliche elektronische Nasen für diese Stoffe zu schaffen. Peratech will es nun geschafft haben, den Erkennungsprozess zu beschleunigen und ein deutlich stärkeres Antwortsignal zu erzeugen, das sich besser auslesen lässt. Die Sensoren sollen nur wenige Mikrometer dünn sein und sich deshalb für zahlreiche Anwendungsfelder eignen. David Lussey, Technikchef bei Peratech: „Dieses neue Sensormedium erlaubt es uns, die VOC-Detektierung in ganz neuen Bereichen einzusetzen, an die früher nicht gedacht werden konnte.“ Eine der Ideen ist, die Sensoren in Schutzkleidung für Ersthelfer einzunähen, die chemisch verunreinigte Orte betreten müssen. Oder die Technik wird einfach in reguläre Alltagskleidung integriert, um den Gesundheitszustand ihres Trägers ständig zu überwachen. Ein besonderes Merkmal der Peratech-Sensoren ist, dass sie sich für den Dünnfilmdruck eignen. Aktuell verfügbare elektronische Nasen erinnern eher an ein Walkie-Talkie. Die Peratech-Sensoren benötigen außerdem nur wenig Strom und könnten mit einer kleinen Batterie versorgt werden, die sich ebenfalls in Kleidung einnähen ließe. Bis zur Vermarktung müssen allerdings noch einige technische Probleme gelöst werden (www.heise.de 23.05.2012).

Rechtsprechung

EuGH

Indirekter Anspruch auf Auskunft über Bewerbungsablehnungsgründe

Der Europäische Gerichtshof (EuGH) entschied mit Urteil vom 19.04.2012 zu der Frage, inwieweit Bewerbende Anspruch gegenüber einem Arbeitgeber haben zu erfahren, warum sie bei einer Stellenbesetzung nicht zum Zug gekommen sind (Az. C-415/10). Zwar bestehe ein solcher Anspruch nicht generell, doch verweigere ein Arbeitgeber „jeden Zugang zu Informationen", so könne das ein Indiz dafür sein, dass eine Diskriminierung vorliege. Nach dem Allgemeinen Gleichbehandlungsgesetz (AGG) von 2006 sind Schadenersatzklagen wegen Diskriminierung deutlich erleichtert. Der Arbeitgeber muss, wenn es Indizien für derartige Diskriminierungen gibt, nachweisen, dass er andere Gründe hatte für die Ablehnung als Geschlecht, Herkunft, Alter, Behinderung oder sexuelle Orientierung der BewerberIn. Deshalb muss er letztlich doch Auskunft geben. Damit begründeten die Richter des EuGH gewissermaßen einen Auskunftsanspruch durch die Hintertür.

Geklagt hatte Galina Meister, Ingenieurin russischer Herkunft, Jahrgang 2001, die sich 2006 erfolglos auf eine Stellenanzeige als Software-Entwicklerin beworben hatte. Als die Stelle erneut ausgeschrieben wurde, wurde ihr wieder abgesagt. Sie fragte nach, ob es einen qualifizierteren Bewerber gegeben habe, doch der Arbeitgeber schwieg. Meister vermutete eine Diskriminierung wegen ihres Geschlechts, Alters oder ihrer Herkunft. Das konnte sie aber nicht beweisen. Der EuGH verlangt nun, dass Bewerbungen nicht aufgrund von - auch unbewussten - Vorurteilen aussortiert werden dürfen, sondern unvoreingenommen geprüft werden müssen. Gründe für eine Ablehnung können z. B. mangelnde Erfahrung, schlechte Noten, Rechtschreibfehler oder unsympathische Selbstdarstellung sein. Der Arbeitgeber muss also keine KandidatIn einladen, von der er weiß, dass er sie nicht einstellen will, es sei denn, die Ablehnung beruht allein darauf, dass es sich z. B. um eine Frau, einen Ausländer oder einen Homosexuellen handelt.

Das Urteil hat zur Folge, dass Arbeitgeber Auswahlverfahren disziplinierter angehen müssen. Bewerbende müssen sich u. U. Unerfreuliches über ihre Qualifikation anhören. Arbeitgebernahe Anwälte kritisierten die EuGH-Entscheidung. Der Bewerbungsprozess werde unnötig aufgebläht. Bewerbende müssten sich zudem häufiger anhören, warum sie ungeeignet seien, was „demotivierend" wirken würde. Dem gegenüber lobte der Direktor des Instituts zur Zukunft der Arbeit, Klaus Zimmermann, das Urteil. Es sei „ein klarer Aufruf an die Unternehmen, ihre Auswahlverfahren bei Stellenausschreibungen transparenter zu gestalten" (Gerichtshof der Europäischen Union, PM Nr. 46/2012 v. 19.04.2012, curia.europa.eu; Kuhr SZ 10.04.2012, 1).

BGH

Verantwortlichkeit eines Hostproviders wegen ehrverletzendem Blog-Eintrag

Der Bundesgerichtshof (BGH) entschied mit Urteil vom 25.10.2011, wie sich von Online-Diffamierungen Betroffene zur Wehr setzen können (Az. VI ZR 93/10; siehe auch, nicht so ausführlich, schon DANA 4/2011, 185). Der Kläger klagte gegen Google als Hostprovider wegen der Verbreitung einer ehrenrührigen Tatsachenbehauptung im Internet auf Unterlassung. Google stellte die technische Infrastruktur und den Speicherplatz für eine Website und für die unter einer Webadresse eingerichteten Weblogs (Blogs) zur Verfügung, auf der ein anonymer Schreiber einen deutschen, auf Mallorca lebenden und arbeitenden Immobilienhändler in deutscher Sprache unter voller Namensnennung unsauberer bis illegaler Geschäftspraktiken verdächtigte und als Pleitier denunzierte. Dieser machte geltend, dies sei unwahr und ehrenrührig.

Das Landgericht Hamburg hatte der Unterlassungsklage hinsichtlich der Verbreitung einer Behauptung im Bereich der Bundesrepublik Deutschland stattgegeben. Die Berufung von Google beim Oberlandesgericht Hamburg hatte insoweit keinen Erfolg. Nach der vom Berufungsgericht zugelassenen Revision entschied der für das Persönlichkeitsrecht zuständige VI. Zivilsenat des BGH, dass im konkreten Fall die deutschen Gerichte international zuständig sind und dass deutsches Recht Anwendung findet (vgl. DANA 2/2011, 89). Zur Frage der Haftung von Google nach deutschem Recht wurde die Sache an das Berufungsgericht zurückverwiesen. Der BGH konkretisierte aber die Voraussetzungen, unter denen ein Hostprovider als Störer für von ihm nicht verfasste oder gebilligte Äußerungen eines Dritten in einem Blog auf Unterlassung in Anspruch genommen werden kann. Danach muss der Hostprovider seine im Folgenden dargelegten Pflichten verletzt haben:

„Ein Tätigwerden des Hostproviders ist nur veranlasst, wenn der Hinweis so konkret gefasst ist, dass der Rechtsverstoß auf der Grundlage der Behauptungen des Betroffenen unschwer - das heißt ohne eingehende rechtliche und tatsächliche Überprüfung - bejaht werden kann. Regelmäßig ist zunächst die Beanstandung des Betroffenen an den für den Blog Verantwortlichen zur Stellungnahme weiterzuleiten. Bleibt eine Stellungnahme innerhalb einer nach den Umständen angemessenen Frist aus, ist von der Berechtigung der Beanstandung auszugehen und der beanstandete Eintrag zu löschen. Stellt der für den Blog Verantwortliche die Berechtigung der Beanstandung sub-

stantiiert in Abrede und ergeben sich deshalb berechtigte Zweifel, ist der Provider grundsätzlich gehalten, dem Betroffenen dies mitzuteilen und gegebenenfalls Nachweise zu verlangen, aus denen sich die behauptete Rechtsverletzung ergibt. Bleibt eine Stellungnahme des Betroffenen aus oder legt er gegebenenfalls erforderliche Nachweise nicht vor, ist eine weitere Prüfung nicht veranlasst. Ergibt sich aus der Stellungnahme des Betroffenen oder den vorgelegten Belegen auch unter Berücksichtigung einer etwaigen Äußerung des für den Blog Verantwortlichen eine rechtswidrige Verletzung des Persönlichkeitsrechts, ist der beanstandete Eintrag zu löschen."

Nach Ansicht des Passauer Professors für Internetrecht Dirk Heckmann enthält die oben zitierte „Checkliste" wachsweiche Kriterien, so dass am Ende sich das Recht von Fall zu Fall entwickeln müsse. Für Google kommentierte deren Konzern-Jurist Haller, in einer Patt-Situation werde sich sein Unternehmen „im Zweifel für die Meinungsfreiheit entscheiden". Google ist groß, finanz- und personalstark. Kleinere Anbieter dürften aber im Zweifel das Prozessrisiko scheuen und einen umstrittenen Eintrag vorsorglich löschen, bevor sie Tausende Euro für Anwälte und Gerichtskosten riskieren. Tatsächlich erhalten die Unternehmen die Funktion eines Schlichters zwischen im Netz Streitenden. Bei einem großen deutschen Hostprovider müssen derartige Konflikte durch das Unternehmen im Monat durchschnittlich fünf Mal entschieden werden. Dabei sind u. U. intimste Details oder Beleidigungen, z. B. gegenüber der einstmals besten Freundin, im Streit. Michael Frenzel von 1&1 beschrieb zusätzlich technische Probleme, die sich beim Provider ergeben können: Bei vielen Servern hätten die eigenen Techniker gar keinen direkten Zugang zu einzelnen Web-Steiten, sondern nur die Mieter des Servers selbst. Im Zweifel müsste der Provider dann den gesamten Server abklemmen, auf dem durchaus 20.000 weitere, unbedenkliche Web-Steiten lagern können.

Fast unmöglich wird eine Selbstverteidigung für Betroffene, wenn es keine Firma gibt, die diese in Anspruch nehmen können, so wie dies im Fall von iShare Gossip der Fall war (vgl. Roth DANA 2/2011, 72ff). Die Betreiber dieser Seite schafften es bis heute, trotz behördlicher Ermittlungen anonym und unbehelligt zu bleiben. Dass die Plattform mittlerweile offline ist, hat nichts mit einsichtigen Providern zu tun. Die Seite war bei der schwedischen Firma PRQ gehostet, die im Ruf steht, auf Bitten von Behörden oder einzelnen Betroffenen nicht zu reagieren. In diesem Fall entschieden die Betreiber offenbar aber selbst, die Seite vom Netz zu nehmen (BGH PM Nr. 169/2011 v. 25.10.2011 juris.bundesgerichtshof.de; Hipp/Müller/Rosenbach Der Spiegel 44/2011, 82).

BGH

Auskunft über IP-Adresse bei praktisch jeder Rechtsverletzung

Der für das Urheberrecht zuständige 1. Zivilsenat des Bundesgerichtshofs (BGH) hat mit Beschluss vom 19.04.2012 entschieden, dass ein Internet-Provider einem Rechteinhaber in aller Regel den Namen und die Anschrift derjenigen Nutzenden einer IP-Adresse mitteilen muss, die ein urheberrechtlich geschütztes Musikstück offensichtlich unberechtigt in eine Online-Tauschbörse eingestellt haben (Az. I ZB 80/11). Die Antragstellerin ist ein Musikvertriebsunternehmen, dem die Naidoo Records GmbH das Recht eingeräumt hat, die Tonaufnahmen des Musikalbums von Xavier Naidoo „Alles kann besser werden" über Online-Tauschbörsen auszuwerten. Sie ließ mit Hilfe eines weiteren Unternehmens die dynamischen IP-Adressen der Deutschen Telekom AG als Internet-Provider ermitteln, über die der Titel „Bitte hör nicht auf zu träumen" des Albums „Alles kann besser werden" im September 2011 in einer Online-Tauschbörse offensichtlich unberechtigt anderen Personen zum Herunterladen angeboten wurde. Die Antragstellerin hat gemäß § 101 Abs. 9 UrhG in Verbindung mit § 101 Abs. 2 Satz 1 Nr. 3 UrhG beantragt, der Deutschen Telekom AG zu gestatten, ihr unter Verwendung von Verkehrsdaten im Sinne des § 3 Nr. 30 TKG über den Namen und die Anschrift derjenigen Nutzer Auskunft zu erteilen, denen die genannten IP-Adressen zu den jeweiligen Zeitpunkten zugewiesen waren.

Das Landgericht Köln hatte den Antrag abgelehnt. Die Beschwerde beim Oberlandesgericht (OLG) Köln blieb ohne Erfolg. Das OLG meinte, die begehrte Anordnung setze eine Rechtsverletzung in gewerblichem Ausmaß voraus, was hier nicht der Fall war. Der BGH hob die Entscheidungen der Vorinstanzen auf und folgte dem Antrag. Eine offensichtliche Rechtsverletzung, im Streitfall das offensichtlich unberechtigte Einstellen des Musikstücks in eine Online-Tauschbörse, begründe einen Anspruch des Rechteinhabers auf Auskunft gegenüber der Telekom als Provider, da sie in gewerblichem Ausmaß für rechtsverletzende Tätigkeiten genutzte Dienstleistungen erbracht hat. Der Anspruch setze nicht voraus, dass die rechtsverletzende Tätigkeit selbst in gewerblichem Ausmaß erfolgt ist. Aus dem Wortlaut des § 101 Abs. 2 Satz 1 Nr. 3 UrhG und der Systematik des Gesetzes ergebe sich eine solche Voraussetzung nicht. Sie widerspräche auch dem Ziel des Gesetzes, Rechtsverletzungen im Internet wirksam zu bekämpfen. Dem Rechteinhaber stünden Ansprüche auf Unterlassung und Schadensersatz nicht nur gegen einen im gewerblichen Ausmaß handelnden Verletzer, sondern gegen jeden Verletzer zu. Er wäre faktisch schutzlos gestellt, soweit er bei Rechtsverletzungen, die kein gewerbliches Ausmaß aufweisen, keine Auskunft über den Namen und die Anschrift der Verletzer erhielte. Wenn ein Auskunftsanspruch besteht, habe das Gericht dem Dienstleister auf dessen Antrag nach § 101 Abs. 9 Satz 1 UrhG zu gestatten, die Auskunft über den Namen und die Anschrift der Nutzer, denen zu bestimmten Zeitpunkten bestimmte IP-Adressen zugewiesen waren, unter Verwendung von Verkehrsdaten zu erteilen. Ein solcher Antrag sei unter Abwägung der betroffenen Rechte des Rechteinhabers, des Auskunftspflichtigen und der Nutzenden sowie unter Berücksichtigung des Grundsatzes der Verhältnismäßigkeit in aller Regel ohne weiteres begründet (SZ 11./12.08.2012, 13; PM BGH Nr. 126/2012 v. 10.08.2012).

LG München I

Anonyme WLAN-Hotspots nicht unzulässig

WLAN-Zugänge, wie es sie in Hotels, Gaststätten, Bahnhöfen und Flughäfen gibt, dürfen weiterhin gemäß einem Urteil des Landgericht München I vom 12.01.2012 anonym angeboten werden (Az: 17 HK O 1398/11). Demnach müssen Anbieter kostenloser Hotspots die Nutzer nicht identifizieren. Gemäß der Mitteilung des AK Vorratsdatenspeicherung ist das Urteil rechtskräftig. Geklagt hatte ein Unternehmen, das in Deutschland WLANs betreibt, in die sich Nutzende mit ihrem eigenen Gerät einloggen können. Dafür müssen sie sich auf einer vorgeschalteten Seite anmelden. Das beklagte Unternehmen bietet ebenfalls WLAN-Hotspots an. In seinen Hotspot-Betreiberverträgen verpflichtet es sich, Vorratsdaten nach EU-Richtlinie zu speichern. Da sich die WLAN-Netze des Beklagten ohne Zugangskontrolle nutzen lassen, werden aber keine Vorratsdaten gespeichert. Der Beklagte lehnte die Aufforderung des Klägers zu speichern ab, weshalb dieser klagte.

Die Klägerpartei sah in der Unterlassung der Identifizierung eine Wettbewerbsverzerrung, Auch wenn das Bundesverfassungsgericht entschieden hat, dass die Speicherung von Verkehrsdaten in der seinerzeit vorliegenden Form in den §§ 113a, 113b TKG nicht verfassungskonform ist, bliebe sie dennoch erforderlich. Die Erhebung von Bestands- und Verkehrsdaten sei nicht verfassungswidrig, die Befugnis ergebe sich aus den §§ 95, 96 des Telekommunikationsgesetzes (TKG). Das Speichern sei auch notwendig, um die Störerhaftung zu vermeiden.

Das Gericht war hingegen der Meinung, die Verpflichtung zur Erhebung und Speicherung der Daten ergebe sich weder aus dem vom Kläger vorgebrachten § 101 UrhG, noch aus den §§ 95, 96, 111 TKG. Das Gericht meinte, anders als der Kläger, dass das Bundesverfassungsgericht nicht nur die Befugnis zur Weitergabe von Vorratsdaten für verfassungswidrig erklärt hatte, sondern auch die Erhebung an sich, und wies die Klage insgesamt ab (www.heise.de 16.07.2012).

OVG Berlin-Brandenburg

Keine Offenlegung der Montblanc-Besteller im Bundestag

Das Oberverwaltungsgericht (OVG) Berlin-Brandenburg wies mit Urteilen vom 07.06.2012 zwei Klagen eines Journalisten eines großen Medienunternehmens ab, der unter Berufung auf das Informationsfreiheitsgesetz des Bundes forderte offenzulegen, welche Abgeordneten sich auf Staatskosten besonders teure Füller bestellt haben (Az. OVG 12 B 34.10 und OVG 12 B 40.11). Das Urteil ist noch nicht rechtskräftig. Das OVG ließ „wegen der grundsätzlichen Bedeutung der Sache“ die Revision beim Bundesverwaltungsgericht zu. Jedes Mitglied des Bundestags kann pro Jahr bis zu 12.000 Euro für Büro- und Geschäftskosten abrechnen. Ende 2009 wurde bekannt, dass sich 115 Abgeordnete Schreibgeräte der Firma Montblanc im Gesamtwert von 68.888 Euro bestellt hatten. Der Journalist wollte nun auch wissen, wer die Besteller waren. Außerdem interessierte er sich für die Anschaffung von Digitalkameras und iPod-Musikabspielgeräten. Doch Namen gab die Verwaltung nicht heraus. Deshalb zog der Redakteur vor Gericht. In erster Instanz entschied das Verwaltungsgericht (VG) Berlin im November 2010, dass die Bundestagsverwaltung das Auskunftsverlangen des Journalisten nochmals zu prüfen habe. Das OVG meinte, die Bundestagsverwaltung könne sich nicht mit Erfolg auf den Schutz von Betriebs- und Geschäftsgeheimnissen und auf einen mit der Informationsbeschaffung verbundenen unverhältnismäßigen Verwaltungsaufwand berufen. Wohl aber hat es den „Schutz mandatsbezogener Informationen“ höher bewertet als das Informationsinteresse der Öffentlichkeit (SZ 08.06.2012, 6; www.focus.de 07.06.2012; Senatsverwaltung für Justiz und Verbraucherschutz Berlin, PM 07.06.2012).

VG Berlin

Verfassungsschutz-Abhörmaßnahmen rechtswidrig

Das Verwaltungsgericht (VG) Berlin hat mit Urteil vom 01.03.2012 in mehreren Verfahren die Rechtswidrigkeit jahrelanger Überwachungsmaßnahmen des Bundesamtes für Verfassungsschutz (BfV) festgestellt (Az. VG A 391.08 u.a.). Seit 1998 bis September 2006 waren Telefonate, E-Mails und Post der Kläger abgehört bzw. überwacht worden. Videokameras wurden vor Haustüren installiert; um einen Sender anzubringen, tauschte das Amt ein Auto mit einem baugleichen Modell aus. Anlass war der vom BfV behauptete Verdacht, die Kläger seien Mitglieder der zur linksautonomen Szene gerechneten sog. „militanten gruppe“ (mg). Der mg wurden mindestens 25 Brandanschläge u. a. auf Polizeiautos und Sozialämter von 2001 bis 2007 zur Last gelegt; Politikern wurden Patronenhülsen geschickt. Schon 2010 hatte der Bundesgerichtshof die polizeilichen Observationen zum Zweck der Strafverfolgung für rechtswidrig erklärt, weil ein „ausreichender Tatverdacht“ nie vorgelegen habe (DANA 2/2010, 79).

Das VG stellte fest, dass die gesetzlichen Voraussetzungen für die Anordnung der Überwachungsmaßnahmen von Anfang an nicht vorlagen. Eingriffe in die Telekommunikationsfreiheit seien nur als letztes Mittel der Aufklärung zulässig, wenn andere Maßnahmen erfolglos geblieben oder von vornherein aussichtslos seien. Bereits im Antrag auf Anordnung der beabsichtigten Überwachungsmaßnahmen beim hierfür zuständigen Bundesministerium des Inneren (BMI) hätte das BfV diese Voraussetzungen bezogen auf den konkreten Sachverhalt darlegen müssen. In seinen Anträgen habe es aber nicht hinreichend konkret begründet, dass die mit den Maßnahmen beabsichtigte Erforschung des Sachverhalts nicht auf andere Weise hätte erfolgen können. Auch hätten keine tatsächlichen Anhaltspunkte für den

vom BfV geäußerten Verdacht vorgelegen, die Kläger gehörten der „militanten gruppe" an. Vielmehr sei aus der Analyse von Verlautbarungen verschiedener Gruppen auf die Identität der Gruppenmitglieder geschlossen worden, ohne dass ein hinreichender Bezug zu den einzelnen Klägern hergestellt worden sei. Auch andere Verhaltensweisen der Betroffenen, wie z. B. zeitweises Nichttelefonieren, habe das BfV ohne weitere konkrete Anhaltspunkte in unzutreffender Weise als tatsächliche Anhaltspunkte für den angenommenen Verdacht angesehen.

Zuvor hatte das BfV, vertreten durch Prof. Heinrich Wolff, die Observationen verteidigt. Es sei Pflicht der Staatsschützer gewesen, nach den schweren Anschlägen alle Spuren zu verfolgen. Die Beschatteten seien langjährig in der linken Szene aktiv gewesen, hätten in Polittexten Wortgruppen benutzt, die auch in Bekennerschreiben der „militanten gruppe" auftauchten. Der Kläger soll als „Antonio" an einem „Runden Tisch der Militanten" über Brandsätze gesprochen haben. Dessen Anwalt Volker Gerloff nannte das „abenteuerliche Konstruktionen". Dass der Kläger „Antonio" sei, habe man nie nachgewiesen. Dennoch seien die Bäckerei, bei er arbeitete und selbst Mandantengespräche zwischen dem Kläger und ihm abgehört worden, „über Jahre und ohne belastbaren Anhaltspunkt. Das ist skandalös".

Jahrelang hatte das BfV keine Ahnung, wer hinter den Bränden der „militante gruppe" steckte. 2007 wurden drei Männer bei einer Brandstiftung gefasst, die 2009 zu Haftstrafen ab drei Jahren verurteilt worden sind. Mit dem 63jährigen Kläger wurde dagegen jahrelang der Falsche beschattet. Dieser kommentierte das Urteil damit, es sei ihm nicht um Revanche gegangen, sondern darum, dem Verfassungsschutz zu zeigen, „dass er nicht alles machen kann, was er will". Die Sache sei ja eine Posse, wäre sie nicht so ernst. Denn während das Amt exzessiv gegen links ermittelte, hätten Nazis unbemerkt gemordet (Senatsverwaltung für Justiz und Verbraucherschutz Berlin PM 9/2012 v. 01.03.2012; Litschko www.taz.de 01.03.2012; SZ 02.03.2012, 8).

VG Berlin

Polizeivideo bei Anti-Überwachungsdemo unzulässig

Das Verwaltungsgericht (VG) Berlin hat das Abfilmen der „Freiheit statt Angst"-Demos 2009 und 2010 für rechtswidrig erklärt (Az. VG 1 K 818.09). Geklagt hatte ein Mitglied des AK Vorratsdatenspeicherung. Die Gruppe organisiert die jährlichen Datenschutz-Demos maßgeblich mit. Das Gericht betonte, dass die Aufzüge laut Versammlungsrecht nur bei „tatsächlichen Anhaltspunkten" für „erhebliche Gefahren für die öffentliche Sicherheit" hätten gefilmt werden dürfen. Dies habe aber bei den „Freiheit statt Angst"-Demos „offensichtlich nicht vorgelegen". Die Kammer bezog sich dabei auf eine Entscheidung vom Juli 2010 (DANA 3/2010, 131 f.). Schon damals hatte das VG das polizeiliche Filmen einer Berliner Anti-Atom-Demonstration für unrechtmäßig erklärt, da diese friedlich verlaufen sei. Demonstranten könnten durch die Kameras „abgeschreckt oder zu ungewollten Verhaltensweisen gezwungen" werden, so die Richter damals.

Die Polizei hatte vor Gericht die Aufnahmen der „Freiheit statt Angst"-Demos verteidigt, indem sie auf Straftaten verwies, die 2009 im Aufzug erfolgt seien. Damals sorgten allerdings vor allem Videos von DemonstrantInnen für Wirbel: Diese hatten einen Polizeiübergriff zweier Beamter auf einen Radfahrer festgehalten. Die PolizistInnen wurden im Mai zu Geldstrafen von 6.000 Euro verurteilt. Peter Ullrich, Forscher am Wissenschaftszentrum Berlin, hat die Folgen von Polizeivideos auf Demos untersucht. Befragte Demo-TeilnehmerInnen äußerten dabei Gefühle von „Ohnmacht und Ausgeliefertsein", so die Studie von 2011. Eine abschreckende Wirkung sei damit gegeben. Reagiert wurde auf die Aufnahmen einerseits mit Verunsicherung, andererseits mit einer „durch Kameras verstärkten Aggression". Letztere führe, so Ullrich, „zu Resistenzverhalten und letztlich einer Ankurbelung der Konfrontation mit der Polizei".

Nach dem ersten Urteil musste der damalige Polizeipräsident Dieter Glietsch im August 2010 eine Weisung erlassen, auf Demos nur bei Straftaten zu filmen. Dies allerdings wird breit ausgelegt: Oft werden Kameras schon bei leichten Unruhesituationen angeschaltet. Auf einer Anti-AKW-Großdemo im März 2009 reichten dafür schon Vermummung und angebliche Gemüsewürfe. Glietsch hatte 2010 auch eine Neuregelung des Versammlungsrechts angeregt, die der Polizei das Filmen grundsätzlich erlaube. Aus der Innenverwaltung hieß es nun, Überlegungen für eine „saubere rechtliche Lösung" seien „noch aktuell".

Die klagenden Datenschützer hatten versucht, auch eine Unterlassung für künftige Aufnahmen zu erwirken. Das wiesen die Richter zurück: Die Weisung, nur bei Straftaten zu filmen, reiche aus. Michael Ebeling vom AK Vorratsdatenspeicherung freute sich dennoch über „das deutliche Urteil". Gleichzeitig nannte er es „bitter", dass „mutige Bürger erst vor Gericht ziehen müssen, um den Behörden den Stellenwert der Meinungs- und Versammlungsfreiheit vor Augen zu führen". Auch der Grüne Benedikt Lux begrüßte die Entscheidung. Das Gericht erkenne damit an, dass das Filmen Demonstranten einschüchtere. SPD-Innenexperte Tom Schreiber sagte, die Konsequenzen aus dem Urteil würden nach der Sommerpause besprochen. Er persönlich sehe bisher „nicht so viele Argumente, warum friedliche Demos gefilmt werden sollten" (Litschko www.taz.de 21.06.2012; PE AK Vorratsdatenspeicherung 22.06.2012, http://www.labournet.de/diskussion/grundrechte/demorecht.html).

VG Bremen

Fragebogen zur Scheineheermittlung rechtswidrig

Das Verwaltungsgericht (VG) Bremen hat mit Beschluss vom 23.05.2012 die verdachtsunabhängige Befragung von Paaren zur „Scheinehenermittlung" mittels umfänglichem Fragebogen in einem Eilverfahren für unrechtmäßig befunden (Az. 4 V 320/12). Der Fragebogen

der Innenbehörde „zur Feststellung der ehelichen Lebensgemeinschaft“ fragt ab, wann der Müll geleert wird und wer auf der linken Seite des Bettes schläft, ob der Gatte Geschenke mitbringt, ab wann genau von einer Beziehung die Rede war oder wie der Kontakt zu den Schwiegereltern ist. 115 Fragen umfasst das Papier, das offiziell als „Verschlusssache“ gehandelt wurde. Ein Türke und seine deutsche Frau hatten den Fragebogen zunächst fast vollständig beantwortet. Später aber beantragten sie die ersatzlose Vernichtung, da der Fragebogen ihr Grundrecht auf informationelle Selbstbestimmung „tiefgreifend“ verletze. Die Ausländerbehörde weigerte sich, die entsprechenden Teile der Akte zu sperren. Hierzu wurde sie nun im Eilverfahren durch das VG verpflichtet.

Das Gericht führte aus, die ausführliche Befragung des Ehepaares und auch die Speicherung der Antworten sei weder durch ein Gesetz noch durch eine Einwilligung der Interviewten gedeckt. Die Speicherung der Antworten sei „möglicherweise bereits von vornherein unzulässig“ – mindestens aber, seit das Ehepaar Einspruch erhob. „Punktuelle Kontrollen“ einer Ehe seien nur bei „begründetem Verdacht“ zulässig. Ermittlungen der Ausländerbehörde seien erst dann erlaubt, wenn „im konkreten Fall tatsächliche Anhaltspunkte“ für eine Scheinehe bestehen, bevor der Fragebogen zum Einsatz kommt: „Eine verdachtsunabhängige Befragung ist unzulässig.“ Gemäß Bundesverwaltungsgericht führen Paare eine „Scheinehe“, wenn sie geheiratet haben, um der ausländischen PartnerIn „ein sonst nicht zu erlangendes Aufenthaltsrecht zu verschaffen“.

Die getrennte Befragung der Eheleute hatte nach der Bewertung der zuständigen Sachbearbeiterin der Ausländerbehörde einen „Anfangsverdacht“ ergeben. Es folgte eine Hausdurchsuchung. Dem gegenüber waren für das VG „Anhaltspunkte“, die den Verdacht einer Scheinehe rechtfertigen würden, „nicht erkennbar“, auch wenn die Ehefrau noch eine Zweitwohnung in einer anderen Stadt und dort auch ein Auto angemeldet hatte. Verdächtig erscheinen den Behörden vor allem solche binationalen Paare, die keine für beide verständliche Sprache sprechen, sich nur „auffallend kurz“ begegnet sind oder bei denen die ausländische PartnerIn zuvor illegal oder nur geduldet in Deutschland gelebt hat.

Die Ausländerbehörde war lediglich bereit, die Antworten auf 11 Fragen zu schwärzen, die von der Landesbeauftragten für Datenschutz beanstandet worden waren. Doch selbst das Schwärzen genügte dem VG nicht: „Schon bei einem einfachen Betrachten der Fragebögen“, so die Entscheidung, scheinen die Antworten durch: „Der Leser ist so ohne Weiteres in der Lage, die Informationen wiederzuerlangen“. Jörg Wegner, Anwalt und Vorsitzender des Verbandes binationaler Familien und Partnerschaften (IAF), sieht in der einstweiligen Anordnung einen „ausdrücklichen Gewinn für unsere Rechtskultur“. Von etwa 2.500 bis 3.000 Ehen, die pro Jahr in Bremen geschlossen werden, ist etwa jede fünfte binational. Bei binationalen Paaren werde in Bremen, so Wegner, „fast grundsätzlich“ eine Scheinehe vermutet. Konkrete Zahlen zu Scheinehen in Bremen konnte zumindest im Jahr 2011 auch der rot-grüne Senat auf Anfrage der Grünen nicht nennen. Der weitere Einsatz der Fragebögen ist unklar: Die Innenbehörde will „die Entscheidung des Gerichts prüfen und dann über die Konsequenzen entscheiden“ (Zier www.taz.de 30.05.2012; ANA-ZAR 3/2012, 21 f.).

BAG

Verdeckte Videoüberwachung zwingt zur Prüfung von Beweisverwertungsverbot

Das Bundesarbeitsgericht (BAG) urteilte am 21.06.2012, dass ein Unternehmen, das sich Beweismittel unter Verletzung gesetzlicher Vorschriften beschafft, diese vor Gericht nicht verwenden darf (Az. 2 AZR 153/11). Gewonnenes Beweismaterial dürfe im Bestreitensfall prozessual „nicht ohne weiteres verwertet werden“. Videoaufzeichnungen müssten datenschutzkonform sein. Das Landesarbeitsgericht muss nun erneut darüber entscheiden, ob die Videoüberwachung im konkreten Fall zulässig oder unzulässig war und deshalb ein Beweisverwertungsverbot besteht, was im zweiten Durchlauf des Kündigungsschutzprozess dann wohl zugunsten der Arbeitnehmerin ausgehen dürfte.

Eine stellvertretende Filialleiterin einer Einzelhandelsfiliale hatte nach mehr als 10 Jahren Betriebszugehörigkeit dem Unternehmen jedenfalls zwei Zigarettenpackungen ohne zu zahlen entwendet. Durch Videoaufzeichnungen konnte das Unternehmen im Kündigungsschutzprozess der Arbeitnehmerin deren Bestreiten des Entwendens widerlegen und den Nachweis führen. Doch war die Videoaufzeichnung vom Unternehmen nicht kenntlich gemacht worden. Zwar rechtfertigt nach Ansicht des BAG der Diebstahl geringwertiger Sachen auch bei 10-jährigem Arbeitsverhältnis eine Kündigung. Doch mit verdeckter Videoüberwachung und -aufzeichnung mit späterer Nutzung in einem Prozess dürfe das Unternehmen nur vorgehen, wenn das Aufklärungsinteresse des Unternehmens (Datenverwendungsinteresse) stärker wiegt als das Geheimhaltungsinteresse der jeweiligen Beschäftigten (informationelles Selbstbestimmungsrecht). Diese Abwägung ginge nur dann zugunsten eines Vorrangs des Unternehmensinteresses und damit zugunsten der verdeckten Videoüberwachung aus, wenn

- der konkrete Verdacht einer strafbaren Handlung oder einer anderen schweren Verfehlung zu Lasten des Arbeitgebers bestünde,
- es keine Möglichkeit zur Aufklärung durch weniger einschneidende Maßnahmen (mehr) gäbe und
- die Videoüberwachung insgesamt nicht unverhältnismäßig gewesen sei

(http://www.datenschutz-berater.de 01.07.2012).

BFH

Steuer-ID für verfassungskonform erklärt

Die Steueridentifikationsnummer (Steuer-ID) verstößt nach einem Urteil des Bundesfinanzhofes (BFH) in

München vom 18.01.2012 nicht gegen das Grundgesetz (Az. II R 49/10). Auch die damit verbundene Speicherung von Daten beim Bundeszentralamt für Steuern ist danach mit der Verfassung vereinbar. Geklagt hatten eine 24-jährige Frau und ihr Kind. Das Gericht stellte zwar fest, dass in das Recht auf informationelle Selbstbestimmung eingegriffen werde. Die Eingriffe in dieses Recht würden aber durch die Interessen des Gemeinwohls überwogen. Indem die Nummern allen Steuerpflichtigen auf Dauer und bundeseinheitlich zugeteilt würden, ermöglichten sie die eindeutige Identifizierung der Personen im Besteuerungsverfahren. Das diene unter anderem dem gleichmäßigen Vollzug der Steuergesetze und ermögliche den Abbau von Bürokratie.

Außerdem könne dem Missbrauch bei Kindergeldanträgen sowie beim Abzug von Kapitalertragssteuer entgegengewirkt werden. Ferner bilden die Identifikationsnummer und die damit verbundene Datenspeicherung nach Überzeugung des Gerichts eine wesentliche Voraussetzung dafür, dass die bisherige Lohnsteuerkarte durch eine elektronische Version ersetzt werden kann. Die Steuer-ID wurde 2007 eingeführt. Mit der jeweils elf Ziffern umfassenden Nummer soll das Besteuerungsverfahren modernisiert und vereinfacht werden. Hierzu erhält das Bundeszentralamt für Steuern von den Meldebehörden elektronisch die im Melderegister gespeicherten sowie die für die Lohnsteuer wichtigen Daten.

Der neue Präsident des BFH Rudolf Mellinghoff hatte erst kurz vor Veröffentlichung des BFH-Urteils seine Zweifel an der Gerechtigkeit des Steuerrechts zum Ausdruck gebracht, das System befände sich in einem „katastrophalen Zustand“. Das deutsche Steuerrecht sei inzwischen so kompliziert, dass man befürchten müsse, dass die Regelungen „nicht mehr gleichmäßig angewendet“ werden könnten. Er bezog sich auf Untersuchungen des Bundesrechnungshofs, die bei Überprüfungen hohe Fehlerquoten der Finanzämter zutage brachten. Wenn selbst die Finanzverwaltung dem komplexen Steuerrecht nicht mehr gewachsen sein, dann müsse man sagen: „Da stimmt was nicht“. Mellinghoff zeigte sich zudem unberührt von den Nichtanwendungserlassen, mit denen die Bundesregierung immer wieder steuerzahlerfreundliche BFH-Entscheidungen aushebelt. Diese Praxis sei unter der aktuellen Regierung seltener geworden: „Und wenn es doch einmal so kommen sollte, dann bin ich selbstbewusst genug, das auch deutlich zu sagen“ (Conradi SZ 02.02.2012, 33; www.rechtslupe.de 02.02.2012; www.rp-online.de 03.02.2012).

FG Niedersachsen

Keine Sammelauskunftspflicht bei ausländischem Internetportal

Das Niedersächsische Finanzgericht (FG) hat die Frage, ob Internetfirmen wie Amazon und Ebay Händlerdaten im großen Umfang an die Steuerbehörden weitergeben müssen, mit Urteil vom 23.02.2012 verneint (Az 5 K 397/10). Die Klage von Amazon gegen ein sogenanntes Sammelauskunftsersuchen der niedersächsischen Steueraufsicht war damit in erster Instanz erfolgreich. Zehntausende von HändlerInnen nutzen Plattformen wie Amazon, um ihre Geschäfte über das Internet abzuwickeln. Die Finanzämter vermuten, dass längst nicht alle von ihnen ihre Erlöse ordnungsgemäß versteuern - und wollten Zugriff auf die Daten erhalten. Die Beamten der niedersächsischen Finanzbehörden forderten von Amazon eine Liste aller landesweiten Anbieter auf dem sogenannten Amazon Marketplace, deren Jahresumsätze über der Kleinunternehmergrenze von 17.500 Euro liegen. Außerdem wollten sie eine detaillierte Auflistung aller Kauf- und Abrechnungsvorgänge, darunter die Art der verkauften Gegenstände, die monatlichen Umsätze und Gesamteinnahmen, eine Aufstellung der Zuschüsse und Gebühren von Amazon und die den Händlern letztlich von Amazon gutgeschriebenen Beträge. Die Behörde versprach sich von der Sammelauskunft Steuernachforderungen in Millionenhöhe. Datenschutzbedenken wiesen sie zurück: Die gewünschten Daten seien sowieso Bestandteil der Buchführung und damit auch im Falle einer Steuerprüfung vorzulegen. Außerdem unterlägen die Finanzbehörden einer strengen Bindung an das Steuergeheimnis.

Im Einzelfall geben Amazon wie auch andere große Handelsplattformen wie Ebay Daten zu verdächtigen HändlerInnen heraus. Doch diese Verdachtsfälle müssen die Fahnder erst einmal identifizieren, bevor sie deren Daten bei den Internetkonzernen anfordern können. Stoßen die Steuerfahnder etwa auf ihren Online-Streifzügen mit speziellen Steuer-Suchmaschinen oder durch den Tipp eines Konkurrenten auf einen dubiosen Händler, schreibt die Finanzbehörde ein Auskunftsersuchen. Das ist ein äußerst mühseliges Vorgehen. Allein bei Amazon, so eine Expertenschätzung, bieten knapp 40.000 Online-HändlerInnen, bei Ebay knapp 30.000 „Powerseller“ ihre Ware an. Für die Behörden äußerst reizvoll: Anbieter wie Amazon zeichnen alle Verkaufsvorgänge minutiös auf.

Das FG beantwortete die Frage nach der Herausgabepflicht an die Steuerfahndung auf banale Art: Weil die Händlerdaten nicht in Deutschland, sondern bei der Amazon-Konzernmutter in Luxemburg liegen, dürfen die deutschen Behörden nicht an sie heran. Die eigentliche Frage um die Zulässigkeit der Sammelauskünfte muss nun in nächster Instanz der Bundesfinanzhof entscheiden. Sollte das Gericht dort zugunsten des Finanzamts urteilen, dürfte Online-Händler eine wahre Flut von Sammelauskunftsersuchen aus dem ganzen Bundesgebiet erwarten – ein Fest der Steuerprüfer. Nach Überzeugung der Steuerfahnder grassiert im Online-Handel der Steuerbetrug. Amazon, Ebay und Co. gelten als die einfachste Möglichkeit, im großen Stil Waren zu verkaufen und die Erlöse schwarz zu kassieren. Als die Hannoveraner Beamten einmal per Einzelauskunftsersuchen Händlerdaten bei Ebay anforderten, brachte das dem Land Niedersachsen letztlich eine zweistellige Millionensumme an zusätzlichen Steuern ein. Das Beispiel soll zeigen, wie viel Steuergeld dem Fiskus beim Online-Handel entgeht und wie einfach das Problem zu lösen wäre. Sollte der Bundesfinanzhof zugunsten der Behörde entscheiden, stünde deut-

schen Online-Händlern eine nie da gewesene Transparenz bevor.

Tatsächlich würden Händler im Internet dann strenger kontrolliert als ihre Offline-Konkurrenz. Die Sammelauskunft entspricht einem ständigen Besuch der Steuerprüfung, konventionelle Ladeninhaber bekommen dagegen nur sehr selten Besuch von den Finanzbeamten. Ein Online-Verkauf von unversteuerten Gütern wäre damit im großen Stil im Internet kaum mehr möglich. Das, so sagen die Fahnder, sei letztlich im Interesse aller anständigen Verkäufer - und damit auch von Amazon. Denn Online-Händler, die schwarz im Internet ihre Waren anbieten, drücken die Preise - und damit auch die 15 Prozent Provision, die sich Amazon von jedem erfolgreichen Kauf nimmt (Knoke www.spiegel.de 01.03.2012).

SG Düsseldorf

Elektronische Gesundheitskarte ist verfassungsgemäß

Das Sozialgericht (SG) Düsseldorf entschied mit Urteil vom 28.06.2012, dass die bereits millionenfach verteilte elektronische Gesundheitskarte (eGK) in ihrer jetzigen Form gesetzes- und verfassungsgemäß sei (Az. S 9 KR 111/09). Ein 32-jähriger, aus Wuppertal stammender Kläger hatte gegenüber der Bergischen Krankenkasse Solingen als Beklagte datenschutzrechtliche Bedenken gegen die beabsichtigte Einführung der eGK erhoben. Der Kläger wird vom Bündnis „Stoppt die E-Card" unterstützt, das von einigen BürgerrechtlerInnen, Patienten- und Ärzteschaftsvertretern getragen wird. Die Datenspeicherung auf der eGK wird gegenüber der bisherigen Krankenversicherungskarte (KVK) so erweitert, dass auf freiwilliger Basis neben den schon heute gespeicherten Daten (wie Name, Anschrift, Gültigkeitsdauer) auch vertrauliche personenbezogene, den Gesundheitszustand betreffende Angaben auf der Karte hinterlegt werden können. Zu diesen Daten gehören z. B. Angaben zur Versorgung im Notfall, ein elektronischer Arztbrief oder Angaben zur Medikamenteneinnahme. Derzeit verfügt der Kläger noch über eine bis zum Ende des Jahres gültige KVK. Der Kläger sah sich in seinem Grundrecht auf informationelle Selbstbestimmung beeinträchtigt und befürchtet, ein „gläserner Patient" zu werden.

Die Kammer hat die Klage abgewiesen. In der mündlichen Urteilsbegründung hat die Vorsitzende ausgeführt, dass der Kläger gegen die Beklagte keinen Anspruch auf Befreiung von der eGK habe. Eine Befreiung von der Pflicht zur eGK sei gesetzlich nicht vorgesehen. Dies sei auch verfassungsrechtlich unbedenklich. Der Versicherte bestimme selbst über die Informationen, die auf der eGK gespeichert würden. Im Hinblick auf Pflichtangaben sei der Kläger nicht beschwert, da diese identisch seien mit den Angaben auf der bisherigen KVK. Nur das Lichtbild sei neu. Die eGK weise im Übrigen nur nach, dass der Kläger in der gesetzlichen Krankenversicherung versichert sei. Der Sachleistungsanspruch des Klägers werde durch die eGK nicht berührt. Im Hinblick auf den konkreten Streitgegenstand gebe es daher keine Veranlassung, auf die (datenschutz-)rechtlichen Bedenken bezüglich der weiteren jedoch freiwilligen und erst zukünftigen Speichermöglichkeiten auf der eGK im Allgemeinen einzugehen. Aufgabe des Gerichts sei nicht die umfassende Prüfung der Rechtmäßigkeit der Einführung der eGK, sondern die konkrete Beschwerde des Klägers. Der Anwalt des Klägers Jan Kuhlmann kündigte an, vor das Landessozialgericht in Berufung zu gehen und bis vor das Bundesverfassungsgericht ziehen zu wollen. Er argumentiert, die Daten seien vor dem unbefugten Zugriff Dritter nicht ausreichend geschützt (vgl. DANA 2/2012, 64 ff.; www.justiz.nrw.de 28.06.2012; www.fr-online.de 28.06.2012).

Mitgliederverteiler

Für diejenigen unter Ihnen, die Informationen über Presseerklärungen u.ä. auf elektronischem Wege bekommen wollten, gab es bisher nur die Möglichkeit, sich in den öffentlich zugänglichen Presseverteiler eintragen zu lassen. Das bestehende Angebot haben wir nun ergänzt und bieten unseren Mitgliedern die Möglichkeit, sich in den neu eingerichteten Mitgliederverteiler aufnehmen zu lassen. Wir werden diesen Verteiler ausschließlich nutzen, um über Aktivitäten der DVD zu berichten.

Damit hierüber nur Mitglieder angesprochen werden, bitten wir Sie im Falle Ihres Interesses, entweder der Geschäftsstelle brieflich oder per Fax eine kurze Nachricht zukommen zu lassen oder per E-Mail an schuler@datenschutzverein.de. Bitte nennen Sie Ihren vollständigen Namen und die E-Mail-Adresse, unter der wir Sie anschreiben sollen. Auch auf der MV im Oktober können Sie Ihre Aufnahme erklären.

Buchbesprechung



Gola/Schomerus,
BDSG, Kommentar,
11. Auflage 2012,
Verlag C. H. Beck,
646 Seiten, € 59,00,

(SH) „Bei der Fertigung der 11. Auflage des Kommentars standen wir vor der Frage, ob hier nicht abgewartet werden sollte bis zur Verabschiedung der seit März 2011 im Gesetzgebungsverfahren befindlichen Vorschriften zum Beschäftigtendatenschutz. Da aber schließlich nicht mehr absehbar war, wann bzw. ob überhaupt das Gesetz verabschiedet wird…" heißt es im Vorwort zur 11. Auflage des Gola/Schomerus. Wie wahr! Die Rechtsentwicklung ist gleichwohl nicht stehen geblieben, und ebenso wenig ist es die Kommentierung im Gola/Schomerus zu § 32 BDSG, der Kernnorm für den Beschäftigtendatenschutz geltenden Rechts. Der Kommentar hat gegenüber der 10. Auflage erfreuliche inhaltliche Ergänzungen und eine prägnantere Gliederung erfahren und arbeitet die relevanten Probleme des Beschäftigtendatenschutzes knapp, aber vollständig und auf der Höhe der Zeit ab. Dabei muss sich das Werk im Wesentlichen auf die Kompetenz des Kommentators für den Beschäftigtendatenschutz, Prof. Gola, stützen. Fachzeitschriften und Rechtsprechung zum Beschäftigtendatenschutz nimmt das Werk nur bis etwa Anfang 2011 auf. Einige jüngere Konsolidierungen in der Rechtsprechung des Bundesarbeitsgerichts, welches sich nunmehr erstmals mit § 32 BDSG zur befassen hatte, finden noch keinen Widerhall.

Behutsame Straffung und sinnvolle Ergänzungen zu Einzelfragen sind auch in anderen Bereichen, etwa zu § 4a BDSG oder im öffentlichen Bereich, der Zweck der neuen Auflage. Struktur und die Tendenz des Gesamtwerks bleiben dagegen unverändert. Auf aktuellstem Stand ist der Bericht über die neueren Entwicklungen in der Gesetzgebung, im Verfassungs- und Europarecht, mit dem die Autorinnen und Autoren das Werk einleiten. Wer sich kurz und knapp über praxisrelevante Fragen zum BDSG orientieren will, wird daher auch mit der 11. Auflage des Gola/Schomeros die nötige Orientierung erfahren- und die Wartezeit bis zu einer gesetzlichen Regelung des Beschäftigtendatenschutzes oder gar einer EU-Datenschutz-Grundverordnung überbrücken können.



Ralf Selig,
Arbeitnehmerdatenschutz,
Logos Verlag, 2011,
183 S., € 36,50

Handreichungen zum Beschäftigtendatenschutz gibt es in großer Zahl. Dass ein Buch zu diesem Thema mit dem Untertitel „Das Datenschutzrecht im Spannungsverhältnis von Mitarbeiterkontrolle und Arbeitnehmerinteressen" an den Markt geht und gleich einen Bogen von den ersten Datenschutzgesetzen in der Bundesrepublik bis zum weiterhin aktuellen Entwurf zur Neuregelung des Beschäftigtendatenschutzes in §§ 32 – 32i BDSG-E spannt, lässt aufhorchen. Das ambitionierte Projekt gelingt aber nur teilweise. Die ersten 83 Seiten verbringt das Werk mit dem Bericht über die Entwicklung des Datenschutzrechts bis ins Jahr 2011, gefolgt von Begriffserklärungen und den Grundzügen des Datenschutzes und Datenschutzrechts in Deutschland. Bis dahin ist von Beschäftigtendatenschutz kaum die Rede. Anschließend folgt die Darstellung des geltenden § 32 BDSG unter Rückgriff insbesondere auf die etablierte Rechtsprechung und Kommentarliteratur. Chancen zu einer weitergehenden und kritischen Annäherung an das Sujet bleiben dabei ungenutzt. Das Werk bleibt im juristischen Duktus gehalten und wirft Fragen auf, um sie danach schulmäßig abzuhandeln. Dabei bemüht sich der Autor um Vollständigkeit, ohne den schon länger auf dem Markt befindlichen Darstellungen des Beschäftigtendatenschutzes etwas hinzuzufügen. Das von einem Juristen für juristisch geprägte Leser geschriebene Buch dürfte für die Akteure in der betrieblichen Praxis keine neuen Vorteile bringen, während die Arbeitsrechtler in der geläufigen Kommentarliteratur und den arbeitsrechtlichen Handbüchern inzwischen eine praxisnähere Orientierung erfahren.

Cartoon

ACTA IST ZWAR GESCHEITETERT, ABER IN DER EU WIRD JA SCHON „CETA", EIN SEHR ÄHNLICHES HANDELSABKOMMEN MIT KANADA VORBEREITET. BREITE MEHRHEITEN WIRD ES DAFÜR SICHER NICHT GEBEN. NUN, DAS KÖNNTE MAN DURCH ABSTIMMUNGEN NACH DEM MUSTER „MELDEGESETZ" LÖSEN. IST NICHT IRGENDWANN WIEDER EINE EUROPA- ODER WELTMEISTERSCHAFT?



Das BKA sucht
Trojaner-Entwickler...
Bundes-Trojaner
eine/n Wissenschaftliche/n Mitarbeiter/in
Kennziffer: BKA-11-2012
als Software Designer/in zur Konzeption und Entwicklung
technischer Überwachungsmethoden bei Straftaten im Zusammenhang
mit Computernetzwerken,
die Vergütung erfolgt außertariflich, vergleichbar der Besoldungsgruppe
A 16 (BBesG)
Der Überwachungsstaat braucht Dich!